User Guide for Resource Manager Essentials

Software Release 4.1
CiscoWorks

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-11714-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

User Guide for Resource Manager Essentials 4.1
Copyright © 1998-2007, Cisco Systems, Inc. All rights reserved.

CONTENTS

Open Source License Acknowledgements xxv

Preface xxix

- Audience xxxi
- Conventions xxxi
- Product Documentations xxxi
- Related Documentation xxxiii
- Obtaining Documentation, Obtaining Support, and Security Guidelines xxxiii

Overview of RME 1-1

- **RME Feature List** 1-1
- Home (Tab) 1-2
  - Device Management Status 1-3
  - Collection Status 1-3
  - Recently Completed Jobs 1-3
  - 24 Hour Syslog Severity Summary 1-4
  - 24 Hour Changes 1-4
  - System Tasks 1-4
  - Device Management Tasks 1-4
  - Reports 1-4
  - Management Tasks 1-5
- Devices (Tab) 1-5
  - Inventory 1-5
  - Device Management 1-6
  - Group Administration 1-8
- Config Mgmt (Tab) 1-8
  - Archive Management 1-8
  - Config Editor 1-10
  - NetConfig 1-11
- Software Mgmt (Tab) 1-11
- Job Mgmt (Tab) 1-13
- Reports (Tab) 1-14
- Tools (Tab) 1-15
  - Change Audit and Audit Trail 1-16
  - Syslog 1-17

NetShow 1-18

Admin (Tab) 1-19

cwcli Framework 1-19

RME Device Center 1-20

RME Process and the Dependency Processes 1-23

Shortcut Links 1-24

What's New in this Release 2-1

New Features in RME 4.1 2-1

Adding and Troubleshooting Devices Using Device Management 3-1

Understanding the Device and Credentials Repository 3-3

Device Management Administration Settings 3-3

Automatic Addition of Device and Credential Repository Devices to RME 3-4

Verifying the Device Credentials While Adding Devices to RME 3-5

Using the RME Devices Window 3-6

Adding Devices to RME 3-7

Licensing Behavior While Adding Devices 3-8

Adding Devices to RME Manually 3-8

Editing Device Attributes While Adding Devices to RME 3-10

Adding Devices to RME Automatically 3-12

Editing RME Device Attributes 3-12

Attribute Error Report 3-16

RME Device Attributes Export File Format 3-16

Exporting RME Device Credentials 3-17

Deleting Devices from RME 3-18

Understanding the RME Device States 3-19

Working With Normal Devices 3-20

Exporting the Normal Devices Credentials 3-21

Suspending the Normal Devices 3-21

Deleting the Normal Devices 3-22

Resubmitting the Normal Devices 3-23

Generating the Inventory and Configuration Collection Status Report 3-23

Working With Pending Devices 3-24

Working With Suspended Devices 3-25

Resubmitting the Suspended Devices 3-26

Deleting the Suspended Devices 3-27

Working With Pre-deployed Devices 3-27

Exporting the Pre-deployed Device Credentials 3-28

Suspending the Pre-deployed Devices 3-29
Deleting the Pre-deployed Devices 3-30
Resubmitting the Pre-deployed Devices 3-31
Diagnosing Pre-deployed Devices 3-31
Working With Alias Devices 3-36
Resolving an Alias Device 3-37
Working With Conflicting Device Types 3-38
Resolving the Conflicting Device Type 3-39
Deleting the Conflicting Device Type 3-40
Checking and Viewing Device Credentials 3-40
Generating Device Credentials Report 3-42
Credential Verification Report 3-42
Credential Error Report 3-44
Verifying Device Credentials 3-44
Viewing Job Details 3-45
Device List Manipulation Service 3-47
XML DTD for DLMS 3-48
Guidelines for Creating the XML File 3-48
Adding Devices to Device Credentials Using DLMS 3-49
Listing the Devices and Their Status Using DLMS 3-50
Getting the Device Credentials Data 3-52
Setting the Device Credentials Using DLMS 3-53
Getting the Device IP Address 3-57
Sample DLMS XML Request File 3-58
Sample Java and PERL Scripts to Invoke the Servlet 3-63
Device Manageability Status 3-67
Understanding Device Manageability Status Report 3-67
Using RME Device Selector 3-68
Using Simple Search 3-70
Using Advanced Search 3-71
Using Advanced Search—An Example 3-75
Using the All Tab 3-76
Using the Search Results Tab 3-78
Using the Selection Tab 3-78
Device Icons and Device Types 3-79

Managing RME Device Groups Using Group Administration 4-1
Using RME Group Administration 4-2
Creating a User-defined Group 4-3

- Entering the Group Properties Details in Properties: Create Dialog Box **4-3**
- Defining the Group Rules in the Rules: Create Dialog Box **4-5**
- Assigning Group Membership in the Membership: Create Dialog Box **4-6**
- Understanding the Summary: Create Dialog Box **4-7**

Editing a User-defined Group **4-8**

Viewing Group Details **4-8**

Viewing Membership Details **4-9**

Refreshing Membership **4-10**

Deleting Groups **4-10**

Understanding the Grouping Rules **4-11**

RME Group Administration Process **4-16**

Understanding RME Device State Transition **5-1**

RME 3.x Behavior **5-1**

States in RME 4.x **5-2**

- State Transitions **5-3**
  - Pending **5-3**
  - Pre-deployed **5-4**
  - Normal **5-4**
  - Aliased **5-4**
  - Suspended **5-4**
  - Conflicting **5-4**
- RME 4.x Scenarios **5-5**
  - Device Addition **5-5**
  - Inventory Detailed Device Report **5-6**
  - Configuration Deployment Using Config Editor **5-6**
  - Configuration Changes Using NetConfig **5-7**
  - Software Image Upgrade **5-8**

Managing Inventory Collection and Polling Using Inventory **6-1**

How to Use Inventory **6-1**

- Pre-requisites **6-2**
- Collecting and Updating Inventory Data **6-2**
- Viewing Reports and Graphs **6-3**

Using the Inventory Job Browser and Viewing Inventory Collection Status **6-4**

- Using the Inventory Job Browser **6-4**
  - Viewing Job Details **6-7**
  - Creating and Editing an Inventory Collection or Polling Job **6-8**
  - Stopping, Cancelling or Deleting an Inventory Collection or Polling Job **6-10**

    - Viewing Inventory Collection Status 6-10
- Inventory Administrative Operations 6-11
    - Setting Change Report Filters 6-12
    - Changing the Schedule for System Inventory Collection or Polling 6-22
    - Cisco.com Fetch Interval 6-23
- Generating Inventory Reports 6-24
    - Generating a 24 Hour Inventory Change Report 6-28
    - Generating a Hardware Report 6-29
    - Generating a Software Report 6-29
    - Generating a Detailed Device Report 6-30
    - Generating a Chassis Slot Summary 6-31
    - Generating Chassis Slot Details 6-31
    - Generating MultiService Port Details 6-31
    - Generating a Hardware Summary Graph 6-32
    - Generating a Software Version Graph 6-32
    - Generating a Chassis Summary Graph 6-33
    - Generating a PSIRT Summary Report 6-33
    - Generating End of Sale/End of Life Report 6-35
- Using Inventory Custom Report Templates 6-38
    - Creating a Custom Report Template 6-38
        - Adding a Rule 6-40
        - Modifying a Rule 6-42
        - Deleting a Rule 6-43
    - Modifying a Custom Template 6-43
    - Deleting a Custom Template 6-44
    - Understanding Template Rules Evaluation 6-44
    - Running a Custom Report 6-45
        - Custom Report Output 6-45
    - Examples of Custom Template Definitions 6-47
        - Template Definition Example 1 6-48
        - Template Definition Example 2 6-48
        - Template Definition Example 3 6-48
        - Template Definition Example 4 6-48
        - Template Definition Example 5 6-48
        - Template Definition Example 6 6-49
        - Template Definition Example 7 6-49
        - Template Definition Example 8 6-49
        - Template Definition Example 9 6-49
        - Template Definition Example 10 6-50

            - Template Definition Example 11 6-50
            - Template Definition Example 12 6-50
    - Using Device Center for Inventory Tasks 6-50

Generating Reports 7-1

- Using the Reports Job Browser 7-1
- Using the Reports Generator 7-4
- Defining Custom Report Templates 7-5
    - Creating a Custom Report Template 7-6
    - Editing a Custom Report Template 7-6
    - Deleting a Custom Report Template 7-6
- Viewing Archived Reports 7-7
- Purging Reports Jobs and Archived Reports 7-8
    - Setting the Reports Archive Default Directory 7-10

Archiving Configurations and Managing Them Using Archive Management 8-1

- Performing Archive Management Tasks 8-1
- Performing Archive Management Administrative Tasks 8-3
- Performing Configuration Management Administrative Tasks 8-3
- Preparing to Use the Archive Management 8-4
    - Entering Device Credentials 8-4
    - Modifying Device Configurations 8-5
        - Enabling rcp 8-5
        - Enabling scp 8-5
        - Enabling https 8-6
        - Configuring Devices to Send Syslogs 8-6
    - Modifying Device Security 8-7
        - Router Commands 8-7
        - Switches Commands 8-7
        - Content Networking—Content Service Switch Commands 8-8
        - Content Networking—Content Engine Commands 8-8
        - Cisco Interfaces and Modules—Network Analysis Modules 8-8
        - Security and VPN—PIX Devices 8-8
- Using Job Approval for Archive Management 8-9
- Configuring Transport Protocols 8-9
    - Requirements to Use the Supported Protocols 8-10
        - Supported Protocols for Configuration Management Applications 8-13
    - Defining the Protocol Order 8-13
- Configuring Default Job Policies 8-14

  - Defining the Default Job Policies 8-14
  - Usage Scenarios When Job Password is Configured on Devices 8-17

Setting Up Archive Management 8-20
  - Moving the Configuration Archive Directory 8-20
  - Enabling and Disabling the Shadow Directory 8-21
  - Configuring Exclude Commands 8-22
  - Configuring Fetch Settings 8-23

Understanding Configuration Retrieval and Archival 8-24
    - Timestamps of Configuration Files 8-25
    - How Running Configuration is Archived 8-25
    - Change Audit Logging 8-26

Defining the Configuration Collection Settings 8-26

Purging Configurations from the Configuration Archive 8-29

Checking Configuration Archival Status 8-31
  - Configuration Archival Reports 8-32
    - Successful Devices Report 8-32
    - Failed Devices Report 8-33
    - Partially Successful Devices Report 8-33

Scheduling Sync Archive Job 8-34

Generating an Out-of-Sync Report 8-36

Scheduling Sync on Device Job 8-37

Using the Configuration Version Tree 8-39

Understanding the Config Viewer Window 8-40

Viewing the Configuration Version Summary 8-42

Configuration Quick Deploy 8-44
  - Performing a Configuration Quick Deploy 8-44

Configuring Labels 8-46
  - Creating a Label 8-47
  - Editing a Labeled Configuration 8-48
  - Viewing the Labeled Configuration 8-49
  - Deleting the Labeled Configuration 8-50

Using Search Archive 8-50
  - Creating a Custom Query 8-51
  - Running a Custom Query 8-52
  - Editing a Custom Query 8-53
  - Deleting the Custom Queries 8-53
  - Searching Archive 8-54
  - Search Archive Result 8-55

Device Configuration Quick View Report 8-56

Comparing Configuration 8-59

Comparing Startup vs. Running Configurations 8-59

Comparing Running vs. Latest Archived Configurations 8-60

Comparing Two Configuration Versions of the Same Device 8-60

Compare Two Configuration Versions of Different Devices 8-61

Understanding the Config Diff Viewer Window 8-63

Using Archive Management Job Browser 8-65

Retrying a Config Job 8-68

Stopping a Config Job 8-70

Deleting the Config Jobs 8-71

Viewing the Archive Management Job Details 8-72

Baseline Template 8-73

Baseline Templates Window 8-76

Creating a Baseline Template 8-77

Creating a Basic Baseline Template 8-77

Creating an Advanced Baseline Template 8-78

Creating an Advanced Baseline Template— Example 8-82

Editing a Baseline Template 8-86

Exporting a Baseline Template 8-87

Importing a Baseline Template 8-87

Deleting a Baseline Template 8-88

Deploying a Baseline Template 8-88

Deploying a Baseline Template Using User Interface 8-89

Deploying a Baseline Template Using File System 8-92

Using Baseline Jobs 8-95

Running Compliance Check 8-96

Understanding the Baseline Compliance Report 8-98

Deploying the Commands 8-99

Deleting the Compliance Jobs 8-103

Making and Deploying Configuration Changes Using NetConfig 9-1

NetConfig Tasks 9-1

Preparing to Use NetConfig 9-2

Verifying Device Credentials 9-2

Modifying Device Security 9-3

Verifying Device Prompts 9-3

Configuring Default Job Policies 9-3

Assigning Task Access Privileges to Users 9-4

    Enabling Job Approval 9-4
Rolling Back Configuration Changes 9-4
    Creating Rollback Commands 9-4
    Configuring a Job to Roll Back on Failure 9-4
Understanding NetConfig User Permissions 9-5
    Job Approval Permissions 9-5
    User-defined Tasks Permissions 9-5
    Administrator Task Permissions 9-5
    Job Editing Permissions 9-5
Using the NetConfig Tab 9-6
Starting a New NetConfig Job 9-6
Browsing and Editing Jobs Using the NetConfig Job Browser 9-11
    Viewing Job Details 9-15
Setting Job Approvers 9-18
Configuring Default NetConfig Job Policies 9-18
Password Policy for NetConfig Jobs 9-18
Setting the Transport Protocol Order for NetConfig Jobs 9-18
Creating and Editing User-defined Tasks 9-18
    Parameterized Templates 9-22
Assigning Tasks to Users 9-25
Handling Interactive Commands 9-26
    Using NetConfig User-defined Templates and Adhoc Tasks 9-26
Handling Multi-line Commands 9-27
Using System-defined Tasks 9-27
    Understanding the System-defined Task User Interface (Dialog Box) 9-30
    Adhoc Task 9-32
    Authentication Proxy Task 9-33
    Banner Task 9-34
    CDP Task 9-35
    Certification Authority Task 9-37
    Crypto Map Task 9-38
    DNS Task 9-40
    Enable Password Task 9-41
    HTTP Server Task 9-43
    Local Username Task 9-44
    IGMP Configuration Task 9-47
    Interface IP Address Configuration Task 9-49
    Internet Key Exchange (IKE) Configuration Task 9-50

    - NTP Server Configuration Task 9-52
    - RADIUS Server Configuration Task 9-53
    - RCP Configuration Task 9-56
    - Reload Task 9-57
    - SNMP Community Configuration Task 9-58
    - SNMP Security Configuration Task 9-60
    - SNMP Traps Configuration Task 9-62
    - Syslog Task 9-67
    - SSH Configuration Task 9-70
    - TACACS Configuration Task 9-72
    - TACACS+ Configuration Task 9-73
    - Telnet Password Configuration Task 9-75
    - Transform System-Defined Task 9-76
    - Web User Task 9-77
    - Use-defined Protocol Task 9-78
    - Cable BPI/BPI+ Task 9-79
    - Cable DHCP-GiAddr and Helper Task 9-80
    - Cable Downstream Task 9-82
    - Cable Upstream Task 9-84
    - Cable Interface Bundling Task 9-87
    - Cable Spectrum Management Task 9-88
    - Cable Trap Source Task 9-90
  - cwcli netconfig 9-91

Editing and Deploying Configurations Using Config Editor 10-1

  - Config Editor Tasks 10-1
  - Benefits of Configuration Editor 10-2
  - Setting Up Preferences 10-7
  - Overview: Editing a Configuration File 10-8
  - Working With the Configuration Editor 10-8
    - Processed Mode 10-9
    - Raw Mode 10-9
    - Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs 10-10
    - Modifying Credentials 10-11
  - Removing a Configuration File 10-12
  - Saving a Configuration File 10-12
  - Undoing All 10-13
  - Replacing All 10-14
  - Printing a Configuration File 10-15

Exporting Changes of a Configuration File 10-15

Deploying a Configuration File 10-16

Closing a Configuration File 10-18

Selecting Configuration Tools 10-18

Comparing Versions of Configuration Files 10-19

Displaying Your Changes 10-20

Overview: Syntax Checker 10-21

Interface to External Syntax Checker 10-21

Registering an External Syntax Checker Application With CMIC 10-22

Viewing the List of Modified Configs 10-23

Overview: Opening a Configuration File 10-24

Opening a Configuration File - By Device and Version 10-24

Opening a Configuration File - By Pattern Search 10-25

Opening a Configuration File - By Baseline 10-27

Baseline Configuration Editor 10-28

Opening an External Configuration File 10-28

What Happens During Configuration Deployment in Overwrite and Merge Modes 10-30

Overview: Downloading a Configuration File 10-30

Starting a New Download Job 10-31

Selecting Configs 10-31

Scheduling a Job 10-32

Configuring Job Policies for Config Editor 10-36

Reviewing the Work Order 10-38

Viewing the Status of all Deployed Jobs 10-39

Using NetShow Commands 11-1

Working With NetShow Jobs 11-2

Viewing the Permission Report 11-2

NetShow Job Browser 11-3

Viewing Job Details 11-5

Masking Credentials 11-7

Creating Jobs 11-7

Editing Jobs 11-10

Copying Jobs 11-13

Stopping Jobs 11-13

Retrying Jobs 11-14

Deleting Jobs 11-14

Archiving NetShow Job Output **11-15**
  Viewing and Analyzing NetShow Output **11-15**
  Deleting Output Archive **11-17**
Command Sets **11-17**
  System-Defined Command Sets **11-18**
Managing Command Sets **11-19**
  Viewing Command Set Details **11-19**
  Creating a New Command Set **11-19**
  Editing Command Sets **11-20**
  Deleting Command Sets **11-21**
  Adding and Deleting Adhoc Commands **11-22**
Assigning Command Sets **11-22**
  Showing Assigned Command Sets **11-23**
  Assigning Command Sets to Users **11-23**
  Assigning Custom Command Execution Privilege **11-23**
Launching show Commands From Device Center **11-24**
Using cwcli netshow Command **11-26**
Administering NetShow Settings **11-26**
  Configuring Job Policies **11-27**
    Defining Default Job Policies **11-27**
    Purging Jobs **11-28**
    Defining Protocol Order **11-29**
  Setting Log Levels **11-30**
  Assigning Approval Lists **11-31**
  Setting Up Job Approval **11-31**
  Generating a Standard Audit Trail Report **11-32**

Managing Software Images Using Software Management **12-1**
Setting Up Your Environment **12-3**
  Requirements on CiscoWorks Server **12-3**
  Logging Into Cisco.com **12-4**
  Using Job Approval for Software Management **12-6**
Software Management Administration Tasks **12-6**
  Viewing/Editing Preferences **12-7**
    Selecting and Ordering Protocol Order **12-10**
    How Recommendation Filters Work for an IOS Image **12-11**
  Updating Upgrade Information **12-13**
Software Repository **12-15**
  Software Repository Synchronization **12-16**

- Scheduling a Synchronization Report 12-17
- Viewing a Synchronization Report 12-18
- Removing a Synchronization Report Job 12-18
- Adding Images to the Software Repository 12-19
- Adding Images to the Software Repository From Cisco.com 12-19
- Adding Images to the Software Repository From Devices 12-22
- Adding Images to the Software Repository From a File System 12-25
- Adding Images to the Software Repository From a URL 12-26
- Adding Images to the Software Repository From the Network 12-28
- Synchronizing Software Image Status With Cisco.com 12-31
- Deleting Images From the Software Repository 12-32
- Exporting of Images from Software Repository 12-32
- Searching for Images From the Software Repository 12-33
- Software Image Attributes 12-33
    - Understanding Software Image Attributes 12-34
    - Understanding Default Attribute Values 12-34
    - Finding Missing Attribute Information 12-35
    - Editing and Viewing the Image Attributes 12-35

Software Distribution 12-36

- Upgrade Analysis 12-37
- Planning an Upgrade From Cisco.com 12-37
- Planning an Upgrade From Repository 12-38
- Understanding the Upgrade Analysis Report 12-39
- Software Distribution Methods 12-41
- Planning the Upgrade 12-42
    - Identifying Possible Changes 12-42
    - Satisfying the Prerequisites 12-42
    - Maintaining Your Software Image Repository 12-43
    - Testing the New Images 12-43
- Configuring Devices for Upgrades 12-44
    - Meeting Minimum Device Requirements 12-44
    - Meeting Additional Device Requirements 12-44
    - Additional SFB Checks 12-45
    - Configuring Telnet and SSH Access 12-45
    - Configuring SCP 12-47
    - Configuring rcp 12-47
    - Configuring TFTP 12-51
    - Configuring HTTP 12-53
    - Meeting Microcode and Modem Firmware Requirements 12-53
- Scheduling the Upgrade 12-53

Authorizing a Distribution Job 12-54

Distributing by Devices [Basic] 12-55

Distributing by Devices [Advanced] 12-59

Distributing by Images 12-64

Support for IOS Software Modularity 12-68

Patch Distribution 12-69

Patch Distribution - by Devices 12-70

Patch Distribution - by Patch 12-73

Remote Staging and Distribution 12-76

Understanding Upgrade Recommendations 12-83

Upgrade Recommendation for Cisco IOS Devices 12-84

Upgrade Recommendation for Catalyst Devices 12-84

Upgrade Recommendation for VPN 3000 Series 12-85

Upgrade Recommendation for Catalyst 1900/2820 12-85

Upgrade Recommendation for Other Device Types 12-86

Using Software Management Job Browser 12-86

Changing the Schedule of a Job 12-88

Retry a Failed Distribution Job 12-88

Undo a Successful Distribution Job 12-89

Stopping a Job 12-90

Deleting Jobs 12-91

Understanding the Software Management Job Summary 12-91

Understanding User-supplied Scripts 12-92

Locating Software Management Files 12-95

Tracking Network Changes Using Change Audit 13-1

How Does it Differ From Syslog? 13-1

Performing Change Audit Tasks 13-2

Performing Maintenance Tasks 13-3

Setting the Purge Policy 13-3

Performing a Forced Purge 13-4

Config Change Filter 13-6

Defining Exception Periods 13-6

Creating an Exception Period 13-7

Enabling and Disabling an Exception Period 13-7

Editing an Exception Period 13-8

Deleting an Exception Period 13-8

Defining Automated Actions 13-8

Understanding the Automated Action Window 13-9

Creating an Automated Action 13-9
Editing an Automated Action 13-11
Enabling and Disabling an Automated Action 13-12
Exporting and Importing an Automated Action 13-12
Deleting an Automated Action 13-13
Using Change Audit Reports 13-13
Generating an Exception Period Report 13-14
Generating 24 Hours and Standard Change Audit Reports 13-16
Understanding Change Audit Report 13-19
ChangeAudit Process 13-20
Stopping and Restarting the Change Audit Process 13-21

Enabling and Tracking Syslogs Using Syslog Analyzer and Collector 14-1
Overview: Common Syslog Collector 14-4
Viewing Status and Subscribing to a Common Syslog Collector 14-5
Viewing Common Syslog Collector Status 14-5
Subscribing to a Common Syslog Collector 14-6
Understanding the Syslog Collector Properties File 14-7
Timezone List Used By Syslog Collector 14-10
Using Syslog Analyzer 14-10
Using Syslog Service on Windows 14-11
Checking the Syslog Configuration File on UNIX 14-12
Stopping and Restarting Syslog Analyzer 14-12
Viewing Syslog Analyzer Status 14-13
Configuring Devices to Send Syslogs 14-13
Configuring the Device Using Telnet 14-14
Configuring the Device Using NetConfig Syslog Task 14-16
Syslog Administrative Tasks 14-18
Setting the Backup Policy 14-19
Setting the Purge Policy 14-20
Performing a Forced Purge 14-21
Defining Custom Report Templates 14-22
Creating a Custom Report Template 14-23
Adding a Message Type 14-24
Deleting a Message Type 14-25
Editing a Message Type 14-25
Selecting a Message Type 14-26
Editing a Custom Template 14-26
Deleting a Custom Template 14-26

Running a Custom Report 14-27

Defining Automated Actions 14-29

Creating an Automated Action 14-30

`Editing an Automated Action 14-32

Guidelines for Writing Automated Script 14-34

Enabling or Disabling an Automated Action 14-34

Exporting or Importing an Automated Action 14-35

Deleting an Automated Action 14-35

Automated Action: An Example 14-36

Verifying the Automated Action 14-37

Defining Message Filters 14-38

Creating a Filter 14-38

Editing a Filter 14-39

Enabling or Disabling a Filter 14-40

Exporting or Importing a Filter 14-40

Deleting a Filter 14-41

Overview: Syslog Analyzer Reports 14-41

Understanding Message Reports 14-44

Generating a 24-Hour Report 14-45

Generating a Syslog Custom Summary Report 14-45

Generating a Severity Level Summary Report 14-45

Generating a Standard Report 14-46

Generating an Unexpected Device Report 14-47

Using Device Center 14-48

Creating a Custom Report: Example 14-48

Prerequisites 14-48

Procedures 14-48

Verification 14-50

Tracking RME Server Changes Using Audit Trail 15-1

Audit Trail Record 15-1

Generating a Standard Audit Trail Report 15-5

Understanding the Audit Trail Report 15-6

Performing Maintenance Tasks 15-7

Setting the Purge Policy 15-7

Performing a Forced Purge 15-8

Checking Bug Status Using Bug Toolkit 16-1

Bug Summary Report 16-1

Logging Into Cisco.com 16-3

Understanding the Bug Summary Report 16-3

Locate Device Report 16-4

Understanding the Locate Device Report 16-7

Working With SmartCase 17-1

Launching Cisco.com Service Request Tool 17-1

Working With Contract Connection 18-1

Accessing and Using Contract Connection 18-1

Getting Device Type Summary Report and Contract Status Detailed Report 18-2

Device Type Summary Report 18-2

Contract Status Detailed Report 18-4

Scheduling Jobs 18-6

Viewing Job Status 18-7

Archiving and Viewing Generated Reports 18-8

CLI Utilities 19-1

CWCLI 19-1

Overview: CLI Framework (cwcli) 19-2

cwcli Global Arguments 19-2

Remote Access 19-4

Overview: cwcli config Command 19-7

Using the cwcli config Command for Batch Processing 19-7

Getting Started With cwcli config 19-7

Uses of cwcli config 19-8

Remote Access 19-10

Running cwcli config 19-10

cwcli config Command Parameters 19-11

Parameters For All cwcli config Commands 19-11

cwcli config Syntax Examples 19-14

cwcli config Core Arguments 19-17

Examples of cwcli config 19-18

cwcli config Command Man Page 19-18

Arguments 19-19

cwcli config Subcommand Man Pages 19-23

Overview: cwcli netconfig Command 19-30

cwcli netconfig Remote Access 19-39

Overview: cwcli export Command 19-40

Using the cwcli export Command 19-41

- Running cwcli export changeaudit 19-45
- Running cwcli export config 19-55
- Running cwcli export inventory Command 19-59
- XML Schema for cwcli export inventory Data 19-60
- Overview: cwcli inventory Command 19-74
  - Using the cwcli inventory Command 19-76
  - Running the cwcli inventory cda Command 19-78
  - Running the cwcli inventory crmexport Command 19-86
  - Running the cwcli inventory deletedevice Command 19-89
  - Running the cwcli inventory getdevicestate Command 19-91
- Overview: cwcli invreport Command 19-93
- Overview: cwcli netshow Command 19-98
  - Running cwcli netshow Command 19-99
  - Executing Netshow CLI Remotely 19-104
- Performance Tuning Tool 19-105
  - PTT Features 19-105
  - Profiles and PTT 19-105
    - Default Profile 19-106
    - Perftune - Windows and Perftune - Solaris 19-106
  - PTT Commands 19-107
- .syslogConf.pl Utility 19-108
- Software Management CLI Utility 19-110
    - Running cwcli swim Command 19-110
    - Executing SWIM CLI Remotely 19-113

Enabling Approval and Approving Jobs Using Job Approval 20-1
- Job Approval Workflow 20-2
- Specifying Approver Details 20-2
- Creating and Editing Approver Lists 20-3
- Assigning Approver Lists 20-4
- Setting Up Job Approval 20-4
- Approving and Rejecting Jobs 20-5
- Job Management 20-8
- RME Job Browser 20-8

Setting System-wide Parameters Using System Preferences 21-1
- Application Log Level Settings 21-1
- Job Purge 21-3
  - Scheduling a Purge Job 21-4

Enabling a Purge Job 21-5

Disabling a Purge Job 21-6

Performing an Immediate Purge 21-6

RME Device Attributes 21-7

RME Secondary Credentials 21-8

Collection Failure Notification 21-9

Configuring Trap Notification Messages 21-10

Examples for Collection Failure Notification 21-10

Fields in a Trap Notification Message 21-11

RME Troubleshooting Tips and FAQs A-1

Device Management A-1

Inventory A-5

Inventory Reports A-15

Archive Management A-21

NetConfig A-28

Config Editor A-30

Software Management A-32

Syslog Analyzer and Collector A-91

Job Approval A-97

Bug Toolkit A-99

cwcli config A-101

cwcli export A-103

NetShow A-105

Administration A-111

Contract Connection A-112

Understanding Syslog Formats B-1

RME Command Reference C-1

Managing Devices When RME Server is Within a NAT Boundary D-1

Configuring RME Server for the NAT Environment D-1

Managing Devices Outside the NAT Boundary D-1

INDEX

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Preface

This document describes the applications that make up Resource Manager Essentials (RME). It provides instructions for configuring, administering, and operating RME.

The Resource Manager Essentials User Guide is organized as follows:

Chapter	Description
Chapter 1, "Overview of RME"	Gives you an overview of RME.
Chapter 2, "What's New in this Release"	Provides you with the list of launch points for the various tasks that you can perform with the various RME applications. You can also review the new features provide for this release.
Chapter 3, "Adding and Troubleshooting Devices Using Device Management"	Describes how RME manages devices. Device Management uses the device credentials that are present in Common Services Device and Credentials database. RME allows you to select devices from Device and Credentials database to manage in RME.
Chapter 4, "Managing RME Device Groups Using Group Administration"	Describes how you can group RME devices. RME allows you to define several groups of devices based on a set of criteria and manage the same.
Chapter 5, "Understanding RME Device State Transition"	Describes how device states are transitioned in RME.
Chapter 6, "Managing Inventory Collection and Polling Using Inventory"	Describes how to use the Inventory application. Inventory, or the Inventory Collection Service (ICS) and Poller software component of RME, collects inventory data from the network devices and keeps the inventory updated.
Chapter 7, "Generating Reports"	Gives you an overview of the reports framework in RME.
Chapter 8, "Archiving Configurations and Managing Them Using Archive Management"	Describes how to use the Configuration Management application. Configuration Management gives you easy access to the configuration files for all files or Cisco IOS-based Catalyst switches, Content Service Switches, Content Engines, and Cisco routers in your RME inventory.
Chapter 9, "Making and Deploying Configuration Changes Using NetConfig"	Describes how to use the NetConfig application. NetConfig allows you to make configuration changes to your managed network devices whose configurations are archived in the Configuration Archive.
Chapter 10, "Editing and Deploying Configurations Using Config Editor"	Describes how to use the Config Editor application. Config Editor you to edit a configuration file that exists in the configuration archive.

Chapter	Description
Chapter 11, “Using NetShow Commands”	Describes how to use the NetShow application. NetShow enables you to define **`show`** commands within Command Sets and run these commands
Chapter 12, “Managing Software Images Using Software Management”	Describes how to use the Software Management application. To ensure rapid, reliable software upgrades, Software Management automates many steps associated with upgrade planning, scheduling, downloading, and monitoring.
Chapter 13, “Tracking Network Changes Using Change Audit”	Describes how to use the Change Audit application. Change Audit tracks and reports changes made in the network. It allows other RME applications to log change information to a central repository.
Chapter 14, “Enabling and Tracking Syslogs Using Syslog Analyzer and Collector”	Describes how to use the Syslog application. Syslog lets you centrally log and track system error messages, exceptions, and other information (such as device configuration changes).
Chapter 15, “Tracking RME Server Changes Using Audit Trail”	Describes how to use the Audit Trail application. Audit Trail tracks and reports changes that the RME administrator makes on the RME server.
Chapter 16, “Checking Bug Status Using Bug Toolkit”	Describes how to use the Bug Toolkit application. Bug Toolkit helps you identify the bugs filed against devices in their network and check the status of the bugs.
Chapter 17, “Working With SmartCase”	Describes how to use the SmartCase application. SmartCase enables you to access Cisco.com from Resource Manager Essentials (RME) to open a Cisco.com case, or to query and update an existing case.
Chapter 18, “Working With Contract Connection”	Describes how to use the Cisco Contract Connection application. Contract Connection lets you verify which of your Cisco devices are covered by a service contract.
Chapter 19, “CLI Utilities”	Describes how to use Command Line Utilities like cwcli, PTT, syslogConf.pl and Software Management CLI.
Chapter 20, “Enabling Approval and Approving Jobs Using Job Approval”	Describes how job approval can be enabled and used.
Appendix A, “RME Troubleshooting Tips and FAQs”	Describes the troubleshooting tips for all the RME applications.
Appendix B, “Understanding Syslog Formats”	Describes the two file formats supported in RME—Comma-Separated Values (CSV) File and XML Schemas.
Appendix C, “RME Command Reference”	Provides a list of the RME commands.
Appendix D, “Managing Devices When RME Server is Within a NAT Boundary”	Describes Network Address Translation (NAT) support in Resource Manager Essentials and provides details of the tasks you need to perform to enable support.

Audience

This document provides descriptions and scenarios for system administrators, network managers, and other users who might or might not be familiar with RME. Many of the tools described are accessible to system administrators only.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentations

The following product documentation is available:

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the Resource Manager Essentials documentation on Cisco.com for any updates.

Release Notes for Resource Manager Essentials

- Release Notes for Resource Manager Essentials on Solaris, Software Release 4.1.
- Release Notes for Resource Manager Essentials on Windows, Software Release 4.1.

These documents are available in the following formats:

- PDF on the LMS 3.0 Documentation CD-ROM.
- On Cisco.com at
  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_release_notes_list.html

User Guide for Resource Manager Essentials 4.1

This document is available in the following formats:

- PDF on the LMS 3.0 Documentation CD-ROM.
- From the Resource Manager Essentials online help.
- On Cisco.com at
  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_list.html

Supported Devices Table

- Supported Devices for Resource Manager Essentials 4.1
- Supported Devices for Software Management Application
- Supported Devices for Configuration Management Application

These documents are available on Cisco.com at
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Context-Sensitive Online Help for Resource Manager Essentials 4.1

You can access the online help by selecting an option from the navigation tree, then click **Help** (extreme right corner of your browser window).

The entire User Guide can be viewed in the Adobe Portable Document Format (PDF) from within the Online Help. To view the PDF, Adobe Acrobat 6.0 or later is required.

The RME device package support for RME is available at install time. You can access the device package help from the Online help.

Step 1 Select an option from RME desktop and click **Help**.

The Help launches in a separate browser window.

Step 2 Click **Main** at the extreme right corner of the page.

The Help window is refreshed and you see these nodes in the left navigation pane:

- CiscoWorks Common Services
- Resource Manager Essentials

Step 3 Expand the Resource Manager Essentials node.

The following leaf and node appear in the left navigation pane:

- RME User Guide (leaf)
- Device Packages (node)

Step 4 Expand the Device Packages node to view the help for device packages.

Related Documentation

Resource Manager Essentials 4.1 runs on Common Services 3.1.

The following related documentation is available in the HTML and PDF formats on Cisco.com at

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/tsd_products_support_series_home.html

- Release Notes for Common Services 3.1 on Solaris.
- Release Notes for Common Services 3.1 on Windows.
- User Guide for Common Services 3.1.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview of RME

The Resource Manager Essentials (RME) suite is part of the CiscoWorks family of products. It is an Enterprise solution to network management. RME is a powerful suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers.

The Resource Manager Essentials browser interface allows easy access to information critical to network uptime and simplifies time-consuming administrative tasks.

RME is based on a client/server architecture that connects multiple web-based clients to a server on the network. As the number of network devices increases, additional servers or collection points can be added to manage network growth with minimal impact on the client browser application.

Taking advantage of the scalability inherent in the intranet architecture, RME supports multiple users anywhere on the network. The web-based infrastructure gives network operators, administrators, technicians, Help Desk staff, IS managers, and end users access to network management tools, applications, and services.

RME allows the network administrators to view and update the status and configuration of all Cisco devices from anywhere on the network through a standard Web browser as the RME client.

RME maintains a database of current network information. It can generate a variety of reports that can be used for troubleshooting and capacity planning. When devices are initially added to the RME, the network administrator can schedule RME to periodically retrieve and update device information, such as hardware, software, and configuration files, to ensure that the most current network information is stored.

In addition, RME automatically records any changes made to network devices, making it easy to identify when changes are made and by whom.

RME applications provide the network monitoring and fault information you need for tracking devices that are critical to network uptime. They also provide tools that you can use to rapidly and reliably deploy Cisco software images and view configurations of Cisco routers and switches.

RME applications, together with links to Cisco.com service and support, automate software maintenance to help you maintain and control your Enterprise network.

You can access RME from CiscoWorks LMS Portal home page. For details, seeWhat's New in this Release. This section lists and introduces you to the new features of RME.

RME Feature List

This section lists all Resource Manager Essentials (RME) applications and the tasks that can be accomplished with each of these applications.

The organization of this section is based on the tabs that are available on the Resource Manager Essentials (**CiscoWorks > Resource Manager Essentials**) page.

- Home (Tab)
- Devices (Tab)
- Config Mgmt (Tab)
- Software Mgmt (Tab)
- Job Mgmt (Tab)
- Reports (Tab)
- Tools (Tab)
- Admin (Tab)
- cwcli Framework
- RME Device Center

This section also lists the RME processes. See RME Process and the Dependency Processes for further details.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Home (Tab)

From this tab, you can access all the frequently used applications in RME, and it also provides the status of some important applications.

The RME Homepage has the following panes:

- Device Management Status
- Collection Status
- Recently Completed Jobs
- 24 Hour Syslog Severity Summary
- 24 Hour Changes
- System Tasks
- Device Management Tasks
- Reports
- Management Tasks

If you check the Auto-Refresh checkbox in the top-left corner of the page, the contents of the page are refreshed at a set interval. You can also click the Refresh icon on the top-right corner of the page to trigger a page refresh.

Device Management Status

This pane gives details about the number of devices in each state, that are managed by RME. This information is fetched from the Device Management page (**RME** > **Devices > Device Management**). You can view the number of devices in the following states in RME: Normal, Pending, Pre-Deployed, Suspended, Alias, and Conflicting. For more details on the device states, see Understanding the RME Device States.

Collection Status

This pane gives details about the collection status for Inventory and Config Archive.

Inventory Collection Status lists the number of successful collections, failed collections, and their details. When you click the hyperlink, it launches the details from the Inventory Collection Status page (**RME > Devices >Inventory > View Inventory Collection Status**).

Config Collection Status lists the number of successful, failed, partially successful, and Out-Of -Sync collections, and their details. When you click the hyperlink, it launches the reports of the failed or partially successful collections. The Out of Sync Summary details are collected from **RME > Config Mgmt >Archive Management > Out-Of-Sync Summary**.

Recently Completed Jobs

This pane shows details of the last eight jobs completed. These details are fetched from the RME Job browser:

Field	Description
Job Id	Unique ID assigned to the job by the system, when the job is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. You can view the job details by clicking on the hyperlink.
Job Type	Reporting application—Bug Toolkit, Change Audit, Contract Connection, Inventory, Syslog, etc.
Status	Status of the scheduled job— Success or Failed. Successful jobs are shown in green, and failed jobs in red.
Description	Description of the job provided by the job creator. (Alphanumeric characters).
Completed At	Date and time the job was completed at.

Click the **More** hyperlink to go to the RME Job browser (**Job Mgmt > RME Jobs**) where you can view the status of all RME jobs.

24 Hour Syslog Severity Summary

This pane gives the Syslog severity message count received in the last 24 hours in the network. It also gives the number for the three severity messages— Emergency, Alerts and Critical from the devices in the network. When you click the message Count hyperlink, the report screens are launched.

24 Hour Changes

This pane gives the number of changes in Config and Inventory in the last 24 hours. When you click the number, a report is displayed with the details for the corresponding devices, with the change category information for the last 24 hours.

System Tasks

This pane provides quick links to the following common system tasks:

- Group Management (**RME >Devices > Group Administration**)
- Device Management (**RME > Devices > Device Management**)
- Sync Archive (**RME > Config Mgmt > Archive Mgmt > Sync Archive**)
- System Inventory Collection (**RME > Admin > Inventory > System Job Schedule**)
- System Config Collection (**RME > Admin > Config Mgmt > Archive Mgmt > Collection Settings**)

Device Management Tasks

This provides quick links to carry out the following common device management tasks:

- Add Device (**RME > Devices > Device Management**)
- Delete Devices (**Common Services > Device and Credentials > Device Management**)
- Edit Device Attributes (**RME > Devices > Device Management > RME Devices > Edit Device Attributes**)
- Import Devices (**Common Services > Device and Credentials > Device Management > Bulk Import**)
- Export Devices (**RME > Devices > Device Management > RME Devices > Export**)

Reports

This pane provides quick links to the following frequently used reports in RME:

- Hardware Report (**RME > Reports > Report Generator**). Hardware Report for Inventory is selected.
- Software Report (**RME > Reports > Report Generator**). Software Report for Inventory is selected.

- Detailed Device Report (**RME > Reports > Report Generator**). Detailed Device Report for Inventory is selected.
- Syslog 24 Hour Report (**RME > Reports > Report Generator**). Syslog 24 Hour Report from Syslog Application is selected.
- Syslog Standard Report (**RME > Reports > Report Generator**). Standard Report from Syslog Application is selected.
- Syslog Severity Level Summary (**RME > Reports > Report Generator**). Severity Level Summary Report from Syslog Application is selected.

Management Tasks

This pane provides quick links to the following common management tasks in RME:

- Netshow—This link takes you to **RME > Tools > NetShow > NetShow Jobs**
- NetConfig—This link takes you to **RME > Config Mgmt > NetConfig > NetConfig Jobs**
- Check Device Attributes—This link takes you to **RME > Devices > Device Management > Device Credential Verification Jobs**
- Edit Config—This link takes you to **RME > Config Mgmt > Config Editor > Config Editor Jobs**
- Config Compliance—This link takes you to **RME > Config Mgmt > Archive Mgmt > Baseline Templates > Baseline Jobs**
- Image Distribution—This link takes you to **RME > Software Mgmt > Software Distribution**.

Devices (Tab)

Networks are a mix of heterogeneous and geographically dispersed systems. Tracking of hardware and software assets in such an environment is very critical. Inventory details and Device Management are basic requirements for all network management applications.

From this tab you can launch these RME applications:

- Inventory
- Device Management
- Group Administration

Inventory

Inventory, or the Inventory Collection Service (ICS) and Poller software component of RME, collects inventory data from the network devices and keeps the inventory updated.

If any changes are detected in hardware or software components, the inventory database will be updated and a change audit record will be created to inform the network manager of the change, and to document the event. This helps to ensure that the information displayed in the Inventory reports reflects the current state of network devices.

Inventory Tasks

You can perform the following tasks using Inventory. See Table 1-1:

Table 1-1 Inventory Tasks

Task	Launch Point
Define filters to customize the data displayed in Inventory change reports.	Resource Manager Essentials > Admin > Inventory > Inventory Change Filter
Schedule system jobs for: • Inventory collection • Inventory polling	Resource Manager Essentials > Admin > Inventory > System Job Schedule
• View, create, and manage Inventory jobs. • View the job details of Inventory jobs (by clicking the Job ID hyperlink in the Inventory Job Browser).	Resource Manager Essentials > Devices > Inventory > Inventory Jobs
View the inventory collection status	Resource Manager Essentials > Devices > Inventory > View Inventory Collection Status
Create and manage Inventory custom report templates.	Resource Manager Essentials > Reports > Custom Report Templates
Create and manage these Inventory reports: • 24 Hour Inventory Change Report • Chassis Slot Details • Chassis Slot Summary • Detailed Device Report • Hardware Report • Software Report • PSIRT Summary Report • End of Sale / End of Life Report • MultiService Port Details • Hardware Summary Graph • Software Version Graph • Chassis Summary Graph	Resource Manager Essentials > Reports > Report Generator. Select the Inventory application and then select the report.

Device Management

Most RME tasks are performed against a set of devices. Device Management is the starting point for all RME applications.

For RME to work with devices, you must first add devices to Common Services Device and Credential Repository. RME provides a facility to either select devices from Device and Credential Repository and add the selected devices into RME or automatically add devices to RME by enabling the Automatically Manage Devices from Credential Repository setting in the Device Management Setting window.

When devices are added to RME, Inventory (and other applications within RME) proceed to contact the device and collect necessary information to be stored in the database.

Device Management Tasks

You can perform the following tasks using Device Management. See Table 1-2:

Table 1-2 Device Management Tasks

Task	Launch Point
Automatically manage devices from Device and Credential database	Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings > Automatically Manage Devices from Credential Repository (option)
Enable check device credentials while adding devices to RME	Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings > Verify Device Credentials While Adding Devices (option)
Select the device credentials that needs to be checked while adding devices to RME.	Resource Manager Essentials > Admin > Device Mgmt > Device Credential Verification Settings
Add devices to RME from Device and Credential Repository. You can also edit the RME device attributes using either Edit Device Attributes or Export and Import buttons.	Resource Manager Essentials > Devices > Device Management > RME Devices > Add Devices button
Editing device attributes (to set different device attributes value for different RME devices.) You can also set the default values for device attributes in the RME Device Attributes window (Resource Manager Essentials > Admin > System Preferences > RME Device Attributes). The values that you enter in this window is applicable to all selected devices in RME.	Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes button
Export RME devices	Resource Manager Essentials > Devices > Device Management > RME Devices > Export button
Check the state of the RME devices.	Resource Manager Essentials > Devices > Device Management
View, export, suspend, resubmit, and delete RME Normal devices. You can also run a Inventory and Configuration Status report using Report button.	Resource Manager Essentials > Devices > Device Management > Normal Devices
View and delete RME Pending devices.	Resource Manager Essentials > Devices > Device Management > Pending Devices
Re-submit and delete the RME suspended devices.	Resource Manager Essentials > Devices > Device Management > Suspended Devices
View, export, suspend, resubmit, and delete RME Pre-deployed devices.	Resource Manager Essentials > Devices > Device Management > Pre-Deployed Devices
Resolve the Alias devices conflict.	Resource Manager Essentials > Devices > Device Management > Alias Devices
Resolve Device Conflicts. You can update the Device and Credentials database or delete conflicting devices.	Resource Manager Essentials > Devices > Device Management > Conflicting Device Types
Schedule Credential Verification jobs.	RME > Devices > Device Management > Device Credential Verification Jobs
View Device Manageability Status	RME > Devices > Device Management > Device Manageability Status

Group Administration

Grouping devices and working with groups provides convenience to you in selecting required devices. You can define several groups of devices based on a set of criteria and manage the same. Device grouping provides an easy way of selecting the required devices.

Group Administration Tasks

You can perform the following tasks using Group Administration. See Table 1-3:

Table 1-3 Group Administration Tasks

Task	Launch Point
Manage RME devices using Device Grouping. You can: • Create a Group • Edit a Group • Delete a Group • View Group Details	Resource Manager Essentials > Devices > Group Administration

Config Mgmt (Tab)

The Configuration Management application stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the RME. It tracks changes to configuration files and updates the database if a change is made.

As the network administrator, you need to be able to control and track changes to device configurations to minimize errors and assist in troubleshooting problems. This can be very difficult if several different users are making changes to the device configurations. It can also become very repetitive and time-consuming. Configuration Management can help simplify and automate these tasks.

From this tab you can launch these Configuration Management applications:

- Archive Management
- Config Editor
- NetConfig

Archive Management

The Archive Management application maintains an active archive of the configuration of devices managed by RME. It provides an,

- Ability to fetch, archive, and deploy the device configurations,
- Ability to handle Syslog triggered config fetches, thereby ensuring that the archive is in sync with the device.
- Ability to search and generate reports on the archived data
- Ability to compare and label configurations, compare configurations with a baseline and check for compliance.

Archive Management Tasks

You can perform the following tasks using Archive Management. See Table 1-4:

Table 1-4 Configuration Management

Task	Launch Point
Set the transport protocol order for Archive Mgmt, NetConfig, and Config Editor jobs.	Resource Manager Essentials > Admin > Config Mgmt.
Enable the job password policy for Archive Mgmt, NetConfig, Config Editor, and cwconfig. You can also configure the default failure job policies.	Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies.
Move the directory for archiving the RME device configuration and enable and disable the usage of Shadow directory.	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt
Purge configuration files from the archive.	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Purge Settings
Check the status of the latest attempt to archive the device configuration.	Resource Manager Essentials > Config Mgmt > Archive Mgmt.
Schedule a job to update the configuration for selected group of devices. The job can be immediate or a periodic job.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive
Generate a Out-of-Sync report for the group of devices whose running configurations differ from their startup configurations.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Out-of-Sync Summary
View all the available configuration versions in the archive for the selected devices.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Version Tree
View the startup, running, or most recently archived configurations, as well as the differences among those configurations.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Version Summary
Search a configuration in the archive by selecting devices and specifying a pattern on which the search has to be performed.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive
Create a Custom Query. You can also: • Run a Custom Query • Edit a Custom Query • Delete the Custom Queries	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive > Custom Queries
Compare two device configuration files from version to version or from device to device.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Compare Configs
Browse the Archive Management jobs that are registered on the system. You can also: • Retry a Config Job • Stop a Config Job • Delete the Config Jobs	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Archive Mgmt Jobs
Create the Label configuration. You can also: • View a Label configuration • Edit a Label configuration • Delete the Label configurations	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Label Configs

Table 1-4 Configuration Management (continued)

Task	Launch Point
Create the Baseline template. You can also: • View a Baseline template • Edit a Baseline template • Delete a Baseline template • Import a Baseline template • Export a Baseline template	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates
Generate a non-compliance configuration report. You can also: • Download this template on to the devices to make it compliant. • Delete the Compliance jobs	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance

Config Editor

The Config Editor application gives you easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file.

Config Editor Tasks

You can perform the following tasks using Config Editor. See Table 1-5:

Table 1-5 Config Editor Tasks

Task	Launch Point
Set or change your Config Editor preferences.	Select RME > Admin > Config Mgmt > Config Editor
View the list of previously opened files in private or public work area.	Select RME > Config Mgmt > Config Editor > Private Configs Or Select RME > Config Mgmt > Config Editor > User Archive
Open a configuration file for editing in four ways: • Device and Version • Pattern Search • Baseline • External Location	Select RME > Config Mgmt > Config Editor > Config Files
View the status of all pending, running, and completed jobs. You can also create a new job or edit, copy, stop and delete a job that you have opened.	Select RME > Config Mgmt > Config Editor > Config Editor Jobs.

NetConfig

NetConfig enables you to make configuration changes to the network devices, whose configurations are archived in the Configuration Archive. It provides easy access to the configuration files for all RME supported devices.

NetConfig Tasks

You can perform the following tasks using NetConfig See Table 1-6:

Table 1-6 NetConfig Tasks

Task	Launch Point
• View and create NetConfig jobs using the NetConfig Job Browser. • View Job details (by clicking the Job ID hyperlink in the NetConfig Job Browser). • You can also: – Edit jobs – Copy jobs – Retry jobs – Stop jobs – Delete jobs	Resource Manager Essentials > Config Mgmt > NetConfig or Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs
Create and manage user-defined tasks.	Resource Manager Essentials > Config Mgmt > NetConfig > User-defined Tasks
Assign user-defined tasks to valid CiscoWorks users.	Resource Manager Essentials > Config Mgmt > NetConfig > Assigning Tasks

Software Mgmt (Tab)

The Software Management application automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network.

The Software Management application provides tools making it easier to store backup copies of all Cisco software images running on network devices. It also helps you to store any additional software images that you may wish to maintain, and to plan and execute software image upgrades to multiple devices on the network at the same time.

It gives you flexibility in upgrading devices with software images. You can either select a set of devices and perform an image upgrade, or select a software image and select a set of devices on which to perform the upgrade. You can even select one of your devices as a remote stage to temporarily store a software image.

It can analyze devices against software image requirements to determine device compatibility and make recommendations before performing a software upgrade.

The Software Management application can also download and list applicable images from Cisco.com, while recommending an image for the device upgrade. You should select the Cisco.com filters in Administration preferences (**Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences**), to avail this benefit.

Software Management Tasks

You can perform the following tasks using Software Management.See Table 1-7:

Table 1-7 Software Management Tasks

Task	Launch Point
You can specify information such as, the directory where images are stored, the pathname of the user-supplied script to run before and after each device software upgrade. You can enable and specify the protocol order for Software Management tasks. You can also enable the Job Based Password option for Software Management tasks. You can specify if the images on Cisco.com should also be included during image recommendation of the device, and also specify the Cisco.com filters so that only those images that match the filter criteria are recommended.	Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences
Upgrade Software Management knowledge base.	Resource Manager Essentials > Admin > Software Mgmt > Update Upgrade Information
Add and delete software images into the software image library using: • Cisco.com • Device • File System • URL • Network You can also update the status of the images using the Update Status button.	Resource Manager Essentials > Software Mgmt > Software Repository
Schedule and generate Synchronization report to find any images running on Software Management-supported devices not in the software image library.	Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization
Determine the impact and prerequisites for a new software deployment using images that reside in Cisco.com and in software image library.	Resource Manager Essentials > Software Mgmt > Software Distribution > Upgrade Analysis

Table 1-7 Software Management Tasks (continued)

Task	Launch Point
Distribute the software images using: • By devices [Basic] • By devices [Advanced] • By image • Use remote staging - by using Staging Device • Use remote staging - by using External TFTP Server	Resource Manager Essentials > Software Mgmt > Software Distribution
• Patch Distribution - by Device • Patch Distribution - by Patch	Resource Manager Essentials > Software Mgmt > Software Distribution> Patch Distribution
Verify your Software Management job status. You can also: • Edit a scheduled Software Management job • Retry a failed Software Management job • Undo a successful Software Management job • Stop a running Software Management job • Delete a Software Management job	Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs

Job Mgmt (Tab)

RME applications, such as NetConfig, Config Editor, Archive Management and Software Management, allow you to schedule jobs to perform their tasks.The Job Approval feature of RME allows you to mandate that one of a group of users designated as job approvers approves each job before it can run.

Job Management Tasks

You can perform the following tasks using Job Management and Job Approval. See Table 1-8:

Table 1-8 Job Management and Job Approval Tasks

Task	Launch Point
Specify and maintain information about users with approver roles.	Resource Manager Essentials > Admin > Approval > Approver Details
Create one or more job approvers list.	Resource Manager Essentials > Admin > Approval > Create/Edit Approver Lists.
Assign approver lists.	Resource Manager Essentials > Admin > Approval > Assign Approver Lists

Table 1-8 Job Management and Job Approval Tasks (continued)

Task	Launch Point
Enable job approval policy for the following applications: • NetConfig • Config Editor • Archive Mgmt • Software Image Mgmt You can enable Job Approval policy for all of these by selecting the All option.	Resource Manager Essentials > Admin > Approval > Approval Policies
View jobs for various applications, using the Job Management browser. For example, Inventory, Syslog, Archive Management, etc.	Resource Manager Essentials > Job Mgmt > RME Jobs
View and approve jobs that are awaiting approval.	Resource Manager Essentials > Job Mgmt > Job Approval

Reports (Tab)

The Reports application provides a new centralized launch point for all report operations, across RME applications.

Reports Tasks

You can perform the following tasks using Reports. See Table 1-9:

Table 1-9 Reports Tasks

Task	Launch Point
Viewing and managing Report jobs, using the Reports Job browser.	Resource Manager Essentials > Reports > Report Jobs
Create, modify or delete custom templates for these applications: • Inventory • Syslog	Resource Manager Essentials > Reports > Custom Report Templates
Create and manage reports for these applications: • Audit Trail • Bug Toolkit • Change Audit • Device Credential • Inventory • Syslog • Contract Connection	Resource Manager Essentials > Reports > Report Generator. Select the required application and then select the report.
View and delete archived reports.	Resource Manager Essentials > Reports > Report Archives.

Table 1-9 Reports Tasks (continued)

Task	Launch Point
Set the reports archive default directory	esource Manager Essentials > Admin > Reports > Archive Settings.
Set the Purge Policy for reports.	Resource Manager Essentials > Admin > System Preferences > Job Purge

You can perform the following tasks using Bug Toolkit. See Table 1-10:

Table 1-10 Bug Toolkit Tasks

Task	Launch Point
Generate a report to view a summary of the software image bugs for a group of devices.	Resource Manager Essentials > Reports > Report Generator Select the Bug Toolkit application and then select the Bug Summary Report.
Search for known bugs that could affect the devices on your network.	Resource Manager Essentials > Reports > Report Generator Select the Bug Toolkit application and then select the Locate Device Report

Tools (Tab)

From, this tab you can launch the following applications:

- Change Audit (Including Audit Trail)
- Syslog
- NetShow
- SmartCase

Change Audit (Including Audit Trail)

The Change Audit application lets you track and report network changes. It provides the capability for other RME applications to log change information to a central repository called the Change Audit log.

The Audit Trail application tracks and reports changes that the RME administrator makes on the RME server. You can generate Audit Trail reports using the Reports tab.

See Change Audit and Audit Trail for more details.

Syslog

The Syslog Analysis application lets you centrally log and track system error messages from Cisco devices. Use logged error message data to analyze router and network performance.

Before you can use Syslog Analysis, you must configure your devices to forward messages either to the RME server directly or to a system on which you have installed a Syslog Analyzer Collector (SAC). The collector filters and forwards the messages to the RME server.

See Syslog for more details.

NetShow

The NetShow application enables you to define **show** commands within Command Sets and run these commands.

You can:

- Create or edit NetShow jobs, using the NetShow job browser. You can also copy, retry, stop, or delete jobs.
- Run a job immediately or schedule it to run at a specified time, once, or periodically.
- Create, edit, or delete user-defined Command Sets.You can also view the details of existing Command Sets.
- Access the stored output that is created from a NetShow job, using the Output Archive.
- Assign one or more Command Sets and Custom Command Execution privilege to one or more users.

See NetShow for more details.

SmartCase

Using SmartCase, you can open/query or update a case on Cisco.com.

To open/query or update a case on Cisco.com, go to **Resource Manager Essentials** > **Tools** > **SmartCase**.

Change Audit and Audit Trail

Change Audit tracks all changes discovered by the Inventory Manager, Software Manager, and Configuration Manager. Every time one of these applications detects a change, it sends a change record to the Change Audit Service, with details of who, when, and what type of change occurred.

Inventory changes include any changes to device information stored in the Inventory database, such as chassis, interfaces, and system information. Software Management changes include upgrades to new software image versions. Configuration Management changes include all changes made to configuration files on devices.

This includes changes made outside of RME tasks, detected by the Configuration Archive process, as well as changes made using RME functionality—NetConfig or Config Editor.

You can perform the following tasks using Change Audit and Audit Trail. See Table 1-11:

Table 1-11 Change Audit and Audit Trail Tasks

Task	Launch Point
Schedule a daily, weekly, or monthly purge job for the Change Audit and Audit trail data.	Resource Manager Essentials > Admin > Change Audit > Set Purge Policy
Schedule a Forced Purge. This purges the Change Audit and Audit trail data immediately or only once.	Resource Manager Essentials > Admin > Change Audit > Force Purge

Table 1-11 Change Audit and Audit Trail Tasks (continued)

Task	Launch Point
Define automated actions on creation of change audit record. You can also: • Creating an Automated Action • Editing an Automated Action • Enabling and Disabling an Automated Action • Exporting and Importing an Automated Action • Deleting an Automated Action	Resource Manager Essentials > Tools > Change Audit > Automated Action
Define an exception period. You can also: • Creating an Exception Period • Editing an Exception Period • Enabling and Disabling an Exception Period • Deleting an Exception Period	Resource Manager Essentials > Tools > Change Audit > Exception Period Definition
Generate Exception Period Report, 24 Hour Report and Standard Report.	Resource Manager Essentials > Reports > Report Generator. Select the Change Audit application and then select the report.
Generate Standard Audit Trail report	Resource Manager Essentials > Reports > Report Generator. Select the Audit Trail application and then select the report.

Syslog

This section describes the tasks that you can perform using Syslog Analyzer and Collector.

Syslog Tasks

You can perform the following tasks using Syslog Analyzer and Collector. See Table 1-12:

Table 1-12 Syslog Analyzer and Collector Tasks

Task	Launch Point
Backup Syslog messages to a CSV (Comma Separated Values) file.	Resource Manager Essentials > Admin > Syslog > Set Backup Policy
Specify a default policy for the periodic purging of Syslog messages.	Resource Manager Essentials > Admin > Syslog > Set Purge Policy
Perform a forced purge of Syslog messages.	Resource Manager Essentials > Admin > Syslog > Force Purge
• View the status of the Common Syslog Collector (to determine if the Collector is reachable or not, etc.) • Subscribe/Unsubscribe to a Common Syslog Collector.	Resource Manager Essentials > Tools > Syslog > Syslog Collector Status

Table 1-12 Syslog Analyzer and Collector Tasks (continued)

Task	Launch Point
• Create automated actions to be executed automatically whenever Syslog Analyzer receives a specific message type. • You can also, – Edit an Automated action – Enable and disable an Automated action – Export and import an Automated action – Delete an Automated action	Resource Manager Essentials > Tools > Syslog > Automated Actions
• Create filters to exclude certain types of Syslog messages from Syslog Analyzer. • Manage filters.	Resource Manager Essentials > Tools > Syslog > Message Filters
Create and manage Syslog custom templates.	Resource Manager Essentials > Reports > Custom Report Templates
Create and manage these Syslog reports: • 24 Hour Report • Custom Summary Report • Severity Level Summary report • Standard Report • Unexpected Device Report	Resource Manager Essentials > Reports > Report Generator. Select the Syslog application and then select the report.

NetShow

This section lists the features and tasks in the Netshow application.

NetShow Tasks

You can perform the following tasks using NetShow. See Table 1-13:

Table 1-13 NetShow Tasks

Tasks	Launch Points
Create or edit NetShow jobs, using the NetShow job browser. You can also copy, retry, stop, or delete jobs. You can run a job immediately or schedule it to run at a specified time, once, or periodically.	Resource Manager Essentials> Tools> NetShow> NetShow Jobs
Access the stored output that is created from a NetShow job using Output Archive.	Resource Manager Essentials> Tools> NetShow> Output Archive

Table 1-13 NetShow Tasks

Tasks	Launch Points
Create, edit, or delete user-defined Command Sets.You can also view the details of existing Command Sets.	Resource Manager Essentials> Tools> NetShow> Command Sets
Assign Command Sets to users. You can assign one or more Command Sets and Custom Command Execution privilege to one or more users.	Resource Manager Essentials> Tools> NetShow> Assigning Command Sets

Admin (Tab)

From this tab, you can perform all RME application administrative tasks such as,

- Set up the backup and purge policies for RME applications.
- Schedule the inventory collection and polling of the devices.
- Define job approval policies.
- Define the upgrade preference for the software image management.
- Set up the Configuration Management job policies
- Automatically manage devices when they are added to DCR.
- Verify credentials of devices when they are added to RME.

In addition to the RME application's administrative tasks you can perform the following tasks. See Table 1-14:

Table 1-14 Admin Tasks

Task	Launch Point
Specify log level settings for all RME applications, or individually.	Resource Manager Essentials > Admin > System Preferences > Loglevel Settings
Schedule, enable or disable purge jobs for RME jobs.	Resource Manager Essentials > Admin > System Preferences > Job Purge
Set the default values for device attributes. These values are applicable to all devices in RME.	Resource Manager Essentials > Admin > System Preferences > RME Device Attributes
Set the Secondary Credentials fall back	Resource Manager Essentials > Admin > System Preferences > RME Secondary Credentials
Configure the receipt of Trap messages by all the hosts mentioned in the env.properties file on Inventory Collection or Config Fetch failure.	Resource Manager Essentials > Admin > System Preferences > Collection Failure Notification

cwcli Framework

cwcli Framework is a command-line interface through which application related functionality is provided.

The framework takes care of the following activities for the applications:

- Parsing the command line for the applications.

- Easy logging and messaging capabilities.
- Authentication and authorization for individual applications.
- Remote access support.

cwcli Framework Commands

The following are the five main commands of cwcli Framework:

```
cwcli config
cwcli export
cwcli inventory
cwcli invreport
cwcli netconfig
cwcli netshow
```

See CLI Utilities for more details.

RME Device Center

Device Center provides a device-centric view for CiscoWorks applications. Device Center is a one-stop place where you can see a quick snapshot summary for a selected device. You can also access various tools, generate reports and perform tasks on the device. You can use Device Center to troubleshoot the device.

From CiscoWorks LMS Portal home page, select **Device Troubleshooting > Device Center** to launch Device Center.

You can perform the following RME tasks using Device Center:

- Summary Pane
- Tools
- Reports
- Management Tasks

Summary Pane

- 24-hour Change Audit Summary

  Displays the changes made in the past 24 hours from the data stored in the Change Audit log.

  Click on the number to launch the Change Audit Standard Report.

  See Generating 24 Hours and Standard Change Audit Reports for further details.
- Inventory Last Collected Time

  Viewing the latest inventory collection status. You can check the time at which inventory was last collected.

  If there is no inventory collection, then a message appears, `No inventory collected yet`.
- Configuration Last Archived Time

  Viewing the latest configuration archived details using the Details link in the Summary (Configuration Last Archived Time) pane

  You can check the time at which configuration was last archived. On clicking the Details link, you can view the differences between the two latest archived running configuration version.

  The Details link appears only if there are two versions of archived running configurations.

If the configuration is not archived, then a message appears, `No configuration archived yet`.

See Understanding the Config Diff Viewer Window for further details.

- 24-hour Syslog Message Summary

  Displays the number of Syslog messages based on the severity that are logged in the past 24 hours.

  - Emergencies—Severity level 0
  - Alerts—Severity level 1
  - Critical—Severity level 2
  - Errors—Severity level 3
  - Warnings—Severity level 4
  - Notifications—Severity level 5
  - Informational—Severity level 6

  Click on the number to launch the Syslog severity report.

  See Generating a Standard Report for further details.

Tools

- Edit Device Credentials

  You can edit the device credentials in the Device and Credential Repository.

  For further information, see section Editing Device Credentials from:

  http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_chapter09186a008053eb1c.html#wp1066043

Reports

- Change Audit Report

  You can generate a Change Audit Standard Report for the device. The Change Audit Standard Report displays all changes that have been logged for the device.

  See Generating 24 Hours and Standard Change Audit Reports for further information.

- Credential Verification Report

  You can generate a Credential Verification Report for the device.

  If there are no credentials to verify a message appears, `None of the devices have credential verification data`. Click on the Check Device Credential link under Management Tasks and then click on Credential Verification Report link under Reports.

  If you had a run a verification report earlier for this device, then this report is displayed.

  See Checking and Viewing Device Credentials for further details.

- Detailed Device Report

  You can generate a device inventory Detailed Device Report.

  See Generating a Detailed Device Report.

- Syslog Messages Report

  You can generate a Syslog Analyzer Standard Report for the device. The Syslog Analyzer Standard Report displays all Syslog messages that have been logged for the device.

  See Generating a Standard Report for further details.

Management Tasks

- Add Images to Software Repository

  You can add software images from the device to the software repository. You can create an immediate image import from device job for the selected device.

  You can check the status of your Image Import (from Device) job by selecting **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

  See Adding Images to the Software Repository From Devices for further details.

- Analyze using Cisco.com Image

  You can determine the impact and prerequisites for a new software deployment using images that reside in Cisco.com.

  See Planning an Upgrade From Cisco.com for further details.

- Analyze using Repository Image

  You can determine the impact and prerequisites for a new software deployment using images that reside in Software Repository.

  See Planning an Upgrade From Repository for further details.

- Check Device Credential

  You have to use this link to trigger the verification process for device credential.

  After performing this task, you should click Credential Verification Report to view the check device credential result.

  See Checking and Viewing Device Credentials for further details.

- Distribute Images

  You can perform a device-centric image distribution. You can create an immediate job to distribute the image.

  You can check the status of your Image Distribution job by selecting **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

  See Distributing by Devices [Basic] for further details.

- Edit Config

  You can edit the device configuration using Config Editor.

  See Working With the Configuration Editor for further details.

- Sync Archive

  You can update the archive. You can create an immediate job to update the configuration archive for the selected device.

  You can check the status of your *Sync Archive* job by selecting **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Archive Mgmt Jobs**.

  See Scheduling Sync Archive Job for further details.

- Update Inventory

  You can update the device inventory. You can create an immediate job to collect the Inventory for the selected device.

  You can check the status of the Inventory Collection job by selecting **Resource Manager Essentials > Devices > Inventory > Inventory Jobs**.

  See Collecting and Updating Inventory Data for further details.

- View Config

  You can view the device configuration. You can create an immediate job to deploy the version of configuration being viewed on the device.

  See Understanding the Config Viewer Window for further details.

- View Pending Jobs

  You can view the pending jobs that are scheduled on the device.

  You cannot view the system-defined jobs, such as *Default config polling job*, *Default config collection job*, etc.

RME Process and the Dependency Processes

The following table lists the Common Services and RME processes and their dependency processes.

If you are stopping or restarting any of the Common Services or RME processes you must stop and restart their dependency processes. You can stop and restart the process using (**Common Services > Admin > Process**). See Table 1-15 for the processes and their descriptions.

Table 1-15 RME 4.1 Process and the Dependency Processes

Process Name	Dependency (Sequential)	Description
RMEDbEngine	None	System service: the database engine for RME applications.
RMEDbMonitor	RMEDbEngine	System service that monitors the accessibility of the RME database engine, which helps to ensure that the system is not started until the database engine is ready.
RMECSTMServer	None.	RMECSTMServer publishes a dummy Common Services Transport Mechanism (CSTM) service name to synchronize publishing of service names with CSTM. All other RME services that publish service names with CSTM are made dependant on this service either directly or indirectly.
ConfigMgmtServer	RMEDbMonitor	Configuration Management service performs the following tasks, • Collects the configuration for the RME managed devices on request from jobs/User Interface. • Archives new version if a change exists between fetched configuration and latest configuration in archive. • Parses the configuration based on configlet rules and generates differences between the configurations. • Logs change record for every new version of archived running configuration. • Detects config changes on the device and triggers configuration collection
NCTemplateMgr	RMEDbMonitor	This service is used to cache the device and NetConfig template mapping information.
NetShowMgr	RMEDbMonitor, RMECSTMServer, EssentialsDM	Populates the database with system-defined command sets and commands by retaining them from device packages.

Table 1-15 RME 4.1 Process and the Dependency Processes (continued)

Process Name	Dependency (Sequential)	Description
RMEOGSServer	**1.** CmfDbMonitor **2.** ESS **3.** RMEDbMonitor	RME group administration service. This is used for managing RME device groups. It is also used for RME device selector.
SyslogCollector	ESS	Filters and sends the syslog objects to various SyslogAnalyzer service subscribed to it.
EssentialsDM	**1.** ESS **2.** DCRServer **3.** RMEDbMonitor	After adding devices to RME, this service triggers for Inventory and Configuration collection.
CTMJrmServer	**1.** RMEDbMonitor **2.** jrm **3.** Tomcat	This service is a proxy to JRM service. This is used by RME application to connect to JRM service. It hides all the direct interaction with JRM.
ChangeAudit	**1.** RMEDbMonitor **2.** CTMJrmServer **3.** jrm	Change Audit program that provides back-end database services for applications that want to log network changes and for Change Audit reports and Automated actions
ICServer	**1.** ESS **2.** CTMJrmServer	This is a service that collects and stores Inventory information from the device using SNMP. It also detects changes that occurred between the last time Inventory was collected for a device, and the current Inventory collection.
SyslogAnalyzer	1. ESS **2.** RMEDbMonitor **3.** CTMJrmServer **4.** jrm	It takes the filter definition from the user and sends it to the various Syslog Collectors it is subscribed to. Receives the syslogs from the Syslog collector and inserts into database and also takes automated actions from the user.

Shortcut Links

You can add shortcuts to frequently used RME links in the CiscoWorks LMS Portal home page. Use these shortcuts to run frequently used tasks/functions.

You can register a URL and add it to either Third Party or Custom Tool menu item to the right of CiscoWorks LMS Portal home page.

For more information on Registering Links With CiscoWorks LMS Portal home page refer to the CiscoWorks Common Services User Guide. To access this, go to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

The additional shortcuts provided in RME are given below.

Note Since some of the URL are long, they are not displayed in a single line in the table. However in the browser the link should be specified in a single line. Hence ensure that the link is displayed appropriately.

For Example: Under Reports section, the link for 24 Hour Inventory Change Report is displayed as below:

http://*RME Server Name:Port No*/rme/CriReportGenerator.do appName%3DInventory%26reportNamereportName%3D24+Hour+Inventory

Where *RME Server Name is the name of the RME server and Port No is the port assigned for RME.*

Function / Task	**URL**
Device Management	
Add a device into DCR	http://*Ciscoworks Server Name:Port No*/rme/cwhp/dcr.device.management.do
RME Device Management	http://*RME Server Name:Port No*/rme/deviceSummary.do
Normal	http://*RME Server Name:Port No*/rme/normaldevices.do
Pending	http://*RME Server Name:Port No*/rme/pendingdevices.do
Pre-deployed	http://*RME Server Name:Port No*/rme/predepdevices.do
Suspended	http://*RME Server Name:Port No*/rme/suspendeddevices.do
Alias	http://*RME Server Name:Port No*/rme/aliasdevices.do
Conflicting	http://*RME Server Name:Port No*/rme/conflictingdevices.do
Check Device Credentials	
Check Device Credentials	http://*RME Server Name:Port No*/rme/cdajobs.do
RME Group Management	http://*RME Server Name:Port No*/rme/ogsMainSetup.do
Reports	
Inventory Reports	
24 Hour Inventory Change Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DInventory%26reportName%3D24+Hour+Inventory
Hardware Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DInventory%26reportName%3DHardware+Report
Software Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DInventory%26reportName%3DSoftware+Report
Chassis Summary Graph	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DInventory%26reportName%3DChassis+Summary+Graph
Detailed Device Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DInventory%26reportName%3DDetailed+Device+Report
Custom Templates	http://*RME Server Name:Port No*/rme/CriCrtm.do
Syslog Reports	
24 Hour Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DSyslog%26reportName%3D24+Hour+Report

Function / Task	URL
Standard Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DSyslog%26reportName%3DStandard+Report
Severity Level Summary Report	http://*RME Server Name:Port No*/rme/rme/CriReportGenerator.do%3FappName%3DSyslog%26reportName%3DSeverity+Level+Summary+Report
Custom Templates	http://*RME Server Name:Port No*/rme/CriCrtm.do
Change Audit Reports	
24 Hour Change Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DChange+Audit%26reportName%3D24+Hour+Report
Standard Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DChange+Audit%26reportName%3DStandard+Report
Exception Period Change Report	http://*RME Server Name:Port No*/rme/CriReportGenerator.do%3FappName%3DChange+Audit%26reportName%3DException+Period+Report
Reports Archive	http://*RME Server Name:Port No*/rme/CriReportArchive.do
Reports Job Browser	http://*RME Server Name:Port No*/rme/CriReportJob.do
Software Image Management	
Software Image Management	http://*RME Server Name:Port No*/rme/swimDefault.do
Image Repository	http://*RME Server Name:Port No*/rme/SwimSlimAction.do
Image Distribution	http://*RME Server Name:Port No*/rme/SwimDistributionAction.do
Jobs	http://*RME Server Name:Port No*/rme/SwimJobMgmtAction.do
Inventory	
Inventory Collection Status	http://*RME Server Name:Port No*/rme/InventoryDefault.do
Inventory Collected	http://R*ME Server Name:Port No*/rme/InventoryCollectionSummary.do%3Faction%3Dcollected
Inventory Never Collected	http://*RME Server Name:Port No*/rme/InventoryCollectionSummary.do%3Faction%3DneverCollected
Jobs	http://*RME Server Name:Port No*/rme/ICSJobBrowser.do
Configuration	
Configuration	http://*RME Server Name:Port No*/rme/configurationDefault.do
Archive Mgmt	
Archive Mgmt	http://*RME Server Name:Port No*/rme/DcmaArchiveSummary.do
Collection Status	http://*RME Server Name:Port No*/rme/DcmaArchiveSummary.do
Successful	http://*RME Server Name:Port No*/rme/DcmaArchiveSummary.do%3Faction%3DSuccess
Failed	http://*RME Server Name:Port No*/rme/DcmaArchiveSummary.do%3Faction%3DFailed
Partial	http://*RME Server Name:Port No*/rme/DcmaArchiveSummary.do%3Faction%3DPartial
Sync Archive	http://*RME Server Name:Port No*/rme/DcmaSyncArchive.do
Out of Sync Summary	http://*RME Server Name:Port No*/rme/DcmaOutOfSync.do

Function / Task	URL
Version Tree	http://*RME Server Name:Port No*/rme/DcmaVersionTree.do
Version Summary	http://*RME Server Name:Port No*/rme/DcmaVersionSummary.do
Search Archive	http://*RME Server Name:Port No*/rme/rme/DCMASearchArchive.do
Compare Configurations	http://*RME Server Name:Port No*/rme/DcmaCompareConfig.do
Label Configs	http://*RME Server Name:Port No*/rme/DcmaLabelConfig.do
Baseline functions	http://*RME Server Name:Port No*/rme/DCMABaseLineConfig.do
Jobs	http://*RME Server Name:Port No*/rme/DcmaJobBrowser.do
Config Editor	
Config Editor	http://*RME Server Name:Port No*/rme/CfgEditStart.do
Config Files	http://*RME Server Name:Port No*/rme/CfgEditOpenConfigMain.do
Private Configs	http://*RME Server Name:Port No*/rme/CfgEditModifiedConfig.do
Public Configs	http://*RME Server Name:Port No*/rme/CfgEditUserConfig.do
Jobs/Create Job	http://*RME Server Name:Port No*/rme/CfgEditJobBrowser.do
Netconfig	
Netconfig	http://*RME Server Name:Port No*/rme/netconfigstart.do
User-defined Tasks	http://*RME Server Name:Port No*/rme/CreateUDT.do
Assign Tasks	http://*RME Server Name:Port No*/rme/assignTask.do
Jobs/Create Job	http://*RME Server Name:Port No*/rme/ncfgJobBrowser.do
Tools	
Tools	http://*RME Server Name:Port No*/rme/toolsDefault.do
Netshow	
Netshow	http://*RME Server Name:Port No*/rme/NetshowStart.do
CommandSets	http://*RME Server Name:Port No*/rme/NetshowCommandSets.do
Output Archive	http://*RME Server Name:Port No*/rme/NetshowOutputArchives.do
Assigning Commandsets	http://*RME Server Name:Port No*/rme/NetshowAssignCommandSets.do
Jobs/Create Job	http://*RME Server Name:Port No*/rme/NetshowJobBrowser.do
Change Audit	
Change Audit	http://*RME Server Name:Port No*/rme/ChangeAuditTools.do
Automated Actions	http://*RME Server Name:Port No*/rme/ChangeAuditAutomatedAction.do
Exception Periods	http://*RME Server Name:Port No*/rme/ChangeAuditExceptionPeriod.do
Syslog	
Syslog	http://*RME Server Name:Port No*/rme/SyslogTools.do
Collector Status	http://*RME Server Name:Port No*/rme/SyslogCollectorStatus.do
Automated Actions	http://*RME Server Name:Port No*/rme/SyslogAutomatedAction.do
Message Filters	http://*RME Server Name:Port No*/rme/SyslogMessageFilter.do
SmartCase	
SmartCase	http://*RME Server Name:Port No*/rme/scOpenCase.do

Function / Task	URL
Administration	
Administration	http://*RME Server Name:Port No*/rme/adminDefault.do
Approver Settings	
Approver Settings	http://*RME Server Name:Port No*/rme/approvalDefault.do
Approver Details	http://*RME Server Name:Port No*/rme/approvalDefault.do
Create/Edit Approver Lists	http://*RME Server Name:Port No*/rme/editL.do
Assigning Approver Lists	http://*RME Server Name:Port No*/rme/assign.do
Approver Policy	http://*RME Server Name:Port No*/rme/preferences.do
Change Audit Settings	
Change Audit Settings	http://*RME Server Name:Port No*/rme/ChangeAuditAdmin.do
Set Purge Policy	http://*RME Server Name:Port No*/rme/ChangeAuditPurge.do
Force Purge Policy	http://*RME Server Name:Port No*/rme/ChangeAuditPurgeNow.do
Config Change Filter	http://*RME Server Name:Port No*/rme/DcmaChangeAuditFilter.do
Config Mgmt Settings	
Config Mgmt Settings	http://*RME Server Name:Port No*/rme/adminConfigManagement.do
Transport Settings	http://*RME Server Name:Port No*/rme/DcmaTransportSettings.do
Archive Mgmt Settings	http://*RME Server Name:Port No*/rme/adminArchiveManagement.do
Config Editor Settings	http://*RME Server Name:Port No*/rme/CfgEditPreferencesSetup.do
Config Job Policies	http://*RME Server Name:Port No*/rme/SavePolicies.do
Device Management Settings	
Device Management Settings	http://*RME Server Name:Port No*/rme/adminDeviceManagement.do
Enable Auto management	http://*RME Server Name:Port No*/rme/dmsettings.do
Verify credential on device addition	http://*RME Server Name:Port No*/rme/dmsettings.do
Credential verification Settings	http://*RME Server Name:Port No*/rme/rmecdasettings.do
Inventory Settings	
Inventory Settings	http://*RME Server Name:Port No*/rme/AdminInventoryDefault.do
Inventory Change Filter	http://*RME Server Name:Port No*/rme/ICSChangeFilter.do
System Job Scheduling	http://*RME Server Name:Port No*/rme/ICSSystemJobSchedule.do
SWIM Settings	
SWIM Settings	http://*RME Server Name:Port No*/rme/SwimAdmin.do
Preferences	http://*RME Server Name:Port No*/rme/SwimAdminAction.do
Upgrade Knowledge base	http://*RME Server Name:Port No*/rme/SwimKBUpgradeAction.do
Syslog Settings	
Syslog Settings	http://*RME Server Name:Port No*/rme/SyslogAdmin.do
Backup Policy	http://*RME Server Name:Port No*/rme/SyslogBackupConf.do
Purge Policy	http://*RME Server Name:Port No*/rme/SyslogPurge.do

Function / Task	**URL**
Force Purge	http://*RME Server Name:Port No*/rme/SyslogPurgeNow.do
System Preferences	
System Preferences	http://*RME Server Name:Port No*/rme/systemPrefDefault.do
Loglevel Settings	http://*RME Server Name:Port No*/rme/rmeLoglevel.do
Purge Jobs	http://*RME Server Name:Port No*/rme/rmeJobPurge.do
Change RME Device Attribute	http://*RME Server Name:Port No*/rme/rmecustomfields.do
RME Job Mgmt	
RME Job Mgmt	http://*RME Server Name:Port No*/rme/rmeJobDflt.do
Jobs Pending for Approval	http://*RME Server Name:Port No*/rme/jobs.do
All RME Jobs	http://*RME Server Name:Port No*/rme/JobMgmtAction.do

CHAPTER 2

What's New in this Release

Resource Manager Essentials 4.1 is the latest release of RME and it forms a part of the Lan Management Solutions (LMS) 3.0 bundle. In addition to the devices supported, this package contains fixes to both existing and newly discovered problems.

For details about the new features in RME 4.1, see New Features in RME 4.1

New Features in RME 4.1

The following are the new features and enhancements in Resource Manager Essentials 4.1:

Support for 10k Devices

The managing capacity of RME is enhanced to support 10k devices with the minimum requirement of Dual CPU and 4GB RAM. A single server with CS 3.1 and RME 4.1 installed in it is equipped with the capacity of managing 10k devices thus optimizing performance and meeting the scalability prerequisite.

The support for 10k devices for RME is applicable only for CW-LMS-3.0-10K-K9 license of LMS 3.0. For more information on licenses, refer to the *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0.*

Support for IOS Software Modularity Images

Cisco IOS Software Modularity images allow the user to apply Maintenance Packs to overcome critical security issues without the need to upgrade to a new software release.

The RME Software Management component allows for distribution of Cisco IOS Software Modularity images as well as Maintenance Packs.

Software Modularity images can be downloaded from Cisco.com to the Software Repository. For detailed hardware support of Software Modularity images please consult the 12.2SX Release Notes.

For more details, see Support for IOS Software Modularity and Patch Distribution.

PSIRT Summary Report

You can use the PSIRT Summary Report to ascertain security vulnerabilities that could affect the devices running IOS in your network. You can generate this Inventory report by selecting this report option from the Report Generator dialog box under RME Reports.

The Cisco.com Fetch Interval option helps you to set the frequency of retrieving PSIRT information from Cisco.com and store it in the RME database.

The Report Generator, retrieves information from this database. It also queries the RME Inventory to retrieve information about the impacted devices and generates the PSIRT Summary Report.

For more details, see Generating a PSIRT Summary Report and Cisco.com Fetch Interval.

End of Sale/End of Life Report

You can use the End of Sale/End of Life Report to ascertain the End of Sale or End of Life details that impact the devices and modules in your network. You can generate this Inventory report by selecting End of Sale/End of Life report option from the Report Generator dialog box under RME Reports.

The Cisco.com Fetch Interval option helps you to set the frequency of retrieving End of Sale/End of Life information from cisco.com and store it in the RME database.

The Report Generator, retrieves information from this database. It also queries the RME Inventory to retrieve information about the impacted devices and modules and generates the End of Sale/End of Life Report.

For more details, see Generating End of Sale/End of Life Report and Cisco.com Fetch Interval.

Performance Tuning Tool

You can tune system parameters using PTT to improve RME performance. Now you can use PTT to tune Sync Archive, NetConfig, Syslog, Device Management, Check Device Attributes (CDA) and Inventory Collection sub systems of the RME application.

For more details, see Performance Tuning Tool.

External TFTP Server Support

The Remote Staging and Distribution now allows you to use an external TFTP server as the staging server, to distribute images to all the devices available in RME. First the image to be distributed is staged to the external TFTP server manually. Then the staged image is upgraded on all the selected devices.

For more details, see Remote Staging and Distribution.

Device Manageability Status

Now you can use this new reporting option to ascertain possible Inventory or Configuration Collection Failure and take timely actions. You can select the required devices and generate an immediate report. This Device Manageability Status report displays the status of Inventory and Configuration Collection.

For more details, see Device Manageability Status.

Dual Supervisor Support

RME Software Image Management now supports upgrading both active and standby supervisor engines or route processors for the following devices: Catalyst 4500, Catalyst 6500 (running Cisco IOS/Cisco IOS Software Modularity), Cisco 7600 Routers, Cisco 10000 Routers.

Secondary Credentials Fallback

The Secondary Credentials page available under System Preferences tab of RME Admin allows you to enable or disable fallback to secondary credentials when authentication through Primary Credentials is not successful.

For more details, see RME Secondary Credentials.

Notification on Inventory / Configuration Failure

You can use the Collection Failure Notification window to configure the receipt of Trap messages on Inventory Collection or Configuration Fetch failure. This Trap is sent for each device from the RME server whenever the collection does not happen.

Other network management stations can use this Trap to know about RME Inventory or Configuration collection failure status. The destination IP address to which the traps are to be sent can be configured in the env.properties file. Any third party Trap receivers in the host(s) mentioned in the env.properties can receive the Trap messages on Config collection/Inventory collection failure.

For more details, see Collection Failure Notification

Netconfig Reload Task

You can use the Reload Task available under RME NetConfig to reload selected devices in one step. This feature can be accessed from both GUI and CLI.

For more details, see Reload Task.

You can use the NetConfig Reload task in conjunction with Software Management (SWIM). During Software Distribution using SWIM, the images are distributed to the selected devices. You can use the **Reload task** to reload those devices for which, you have not selected **Reboot immediately after download** option while scheduling the distribution of the images.

Syslog Support for CSS Devices

From this release, the CSS Syslog messages are also supported.

Software Management Command Line Interface (SWIM CLI)

You can use the new SWIM CLI utility to list software images available in the Software Management Repository as well as export images from the Software Management Repository.

For more details, see Software Management CLI Utility.

CWCLI Support for CDA Jobs

The CDA jobs are now provided CWCLI support. Apart from using the GUIs for CDA jobs, you can use CWCLI to create, list, stop, cancel, delete CDA jobs as well as verify the CDA job status.

For more details, see Running the cwcli inventory cda Command.

GUI Based Write2Start Option

The Write2Start option can now be executed from both CLI and GUI.

For more details, see **Push Config To** field description in Scheduling a Job.

Enhanced Severity Level Summary Report

This report has been enhanced to provide more comprehensive details about the syslogs for each severity for each device. The syslogs are categorized based on severities as Emergencies, Alerts, Criticality, Errors, Warnings, Notifications, Informational messages and Debug messages.

For each device, count of syslogs is provided for each severity. Clicking on any severity count link corresponding to a device, in the report provides detailed information about the messages for that severity.

For more details, see Generating a Severity Level Summary Report.

GUI Based Option to Export Images from Software Repository

Now you can export software images from Software Repository using the GUI based Export button. For more details, see Exporting of Images from Software Repository.

SysUpTime Attribute for Inventory Custom Reports

SysUpTime is a new attribute added for Inventory Custom Reports.

For more information, see the attributes under the System Report Inventory Group in Adding a Rule.

CHAPTER 3

Adding and Troubleshooting Devices Using Device Management

For RME to work with devices, you must first add devices to Common Services Device and Credential Repository. Once a device is added to the Device and Credential Repository, you can then add it to the RME.

You can add devices from the Device and Credential Repository to RME automatically by enabling Automatically Manage Devices from Credential Repository (by default, this is enabled), or you can add them selectively by disabling the Automatically Manage Devices from Credential Repository setting in the Device Management Setting window.

For more information on how to add devices to RME, see Adding Devices to RME.

After you have added the devices to RME, RME applications such as Configuration Management, Inventory, and Software Management will use the credentials stored in Device and Credential Repository.

You can perform the following tasks using RME Device Management:

- Adding devices to RME from Common Services' Device and Credential Repository.

  You can add devices to RME only after adding devices to Common Services' Device and Credential Repository.

  You can also check the device credentials while adding devices by selecting the check box, Verify Device Credentials While Adding Devices on Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**).

  See Adding Devices to RME for further details.

- List RME devices

  Displays all RME devices and their respective states.

  See Understanding the RME Device States for further details.

- Delete RME Devices

  Delete devices, including all related device information, that you no longer track.

  See Deleting Devices from RME for further details.

- Change Device Credentials for RME Devices

  A launch point is provided in RME to update device information that is present in Device and Credential Repository. You can edit these credentials, SNMP read and write community strings, Telnet and console-enable passwords, TACACS and local usernames and passwords.

- Exporting Device Credentials for RME Devices

Export the device credentials for RME devices in CSV 3.0 and XML file formats.

See Exporting RME Device Credentials for further details.

- Check Device Credentials on RME Devices

  Verify that Device and Credential Repository credentials match actual device credentials. This includes SNMP read and write community strings, Telnet and console-enable passwords, and TACACS and local usernames and passwords.

  You can automatically check device credentials when you add or import devices.

  See Checking and Viewing Device Credentials for further details.

- Setting the RME Device Attributes

  Set the default device attributes in RME such as Serial Number, SNMP timeout, SNMP retry, Telnet timeout, TFTP Timeout, and Natted RME IP Address.

  See Editing RME Device Attributes for further details.

- Using RME Device Selector

  Select the RME devices to perform the different RME tasks.

  See Using RME Device Selector for further details.

- Set the debug mode for RME Device Management and Device Selector applications

  You can set the debug mode for RME Device Management and Device Selector applications in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

  See Application Log Level Settings for further details.

- Perform the Device Status Test

  You can verify the Device Status to find means to troublshoot Inventory and Config failure.

  See Device Manageability Status for further details.

- Using Device Center you can perform the following Device Management tasks:
  - Check device credentials
  - Generate Device Credential Verification report

  See RME Device Center for further details.

You can perform the following tasks using the command line utility:

- You can check the specified device credentials for the RME devices using **`cwcli inventory cda`**.
- You can export device credentials of one or more RME devices in clear text using **`cwcli inventory crmexport`**.
- You can delete the specified RME devices using **`cwcli inventory deletedevice`**.
- You can view the RME devices state using **`cwcli inventory getdevicestate`**.

See Overview: cwcli inventory Command for further details.

You can perform the following tasks using the Device List Manipulation Service:

- Add devices
- List the RME devices and their status
- Get the device credentials data
- Set the device credentials data

- Get the device IP address

See Device List Manipulation Service for further details.

For the new features in this release, see "What's New in this Release".

Understanding the Device and Credentials Repository

The Device and Credential Repository is part of Common Services application. This is a centralized device repository for sharing device credentials across all applications that are installed on CiscoWorks server.

Use the Device and Credential Repository (**Common Services > Device and Credentials > Device Management**) to:

- Add a device
- Edit device identity
- Import bulk devices
- Edit device credentials
- View the list of devices on CiscoWorks server

You can also, export and delete devices in Device and Credential Repository.

You cannot add devices directly to the RME. You must first add the devices to the Common Services' Device and Credential Repository and then import the devices to RME.

The RME application uses these device credentials from the Device and Credential Repository:

- Device identity information such as IP address/host name.
- Device access information such as user names/passwords and SNMP community strings.

When a device is deleted from RME, the Device and Credential Repository is not affected. You can selectively add the devices back to RME. If a device is deleted from Device and Credential Repository, the device is also deleted from the RME application.

For more information on the Device and Credential Repository, see the *Common Services Online Help* and *User Guide*.

Device Management Administration Settings

Before adding devices to RME you can set these Device Management Settings for:

- Automatically adding devices to RME from Device Credentials Repository

  Select the check box *Automatically Manage Devices from Credential Repository* on Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt**).

  See Automatic Addition of Device and Credential Repository Devices to RME.

  This option is enabled by default. If you want to manually add device to RME, then disable this option.

  See Adding Devices to RME Manually

- Verifying the device credentials while adding devices to RME

Select the check box *Verify Device Credentials While Adding Devices* on Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt**).

See Verifying the Device Credentials While Adding Devices to RME.

- Selecting the device credentials that need to be verified while adding devices to RME

  Select the device credentials using **Resource Manager Essentials > Admin > Device Mgmt > Device Credential Verification Settings**.

  See Verifying the Device Credentials While Adding Devices to RME.

Automatic Addition of Device and Credential Repository Devices to RME

Whenever you add devices to Common Services' Device and Credential Repository, RME triggers the Device Auto Management service. The devices that are added to Device and Credential Repository gets added to RME automatically.

This service is enabled by default. That is, once you have added device to Device and Credential Repository then automatically the devices get added to RME.

The Device Auto Management service gets triggered only when you add devices to Common Services Device and Credential Repository through,

- User interface (**Common Services > Device and Credentials > Device Management**)
- Command line tool `dcrcli`

This service is not triggered when you upgrade a CiscoWorks license file.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To enable the Device Auto Management setting:

Step 1 Select **Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**.

The Device Management Settings dialog box appears.

Step 2 Select **Automatically Manage Devices from Credential Repository**.

Step 3 Click **OK**.

If any new devices are added in Device and Credential Repository (**Common Services** > **Device and Credentials** > **Device Management**) these devices are also added in RME automatically.

If there are any devices that are deleted from RME before enabling this option, those devices are not added to RME. You have to add those devices to RME manually. See Adding Devices to RME Manually.

Select either:

- **Resource Manager Essentials > Devices > Device Management** to view the RME device state.

  or

- **Resource Manager Essentials > Devices > Device Management > RME Devices** to view the RME devices.

Verifying the Device Credentials While Adding Devices to RME

You can check your device credentials while adding devices to RME and view the results in a report. Use this option to make sure that your Device and Credential Repository credentials, match your actual device credentials.

Verifying device credentials while adding devices to RME involve:

1. Selecting the credentials that need to be verified while adding devices to RME.
2. Selecting the verify device credentials while adding devices.
3. Viewing the credentials verification report.

Before performing Step 3, you must add devices to RME. See Adding Devices to RME to add devices to RME.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To select the credentials that need to be verified while adding devices to RME:

Step 1 Select **Resource Manager Essentials > Admin > Device Mgmt > Device Credential Verification Settings**.

The Device Credential Verification Settings dialog box appears.

Step 2 Select the credentials that need to be checked.

You can check the following device credentials:

- SNMP Read Community String—SNMP version 2 read community string.
- SNMP Write Community String—SNMP version 2 write community string.
- SNMPv3—SNMP version 3 username and password
- Telnet—Telnet username and password.
- Telnet Enable Mode User Name and Password—Telnet username and password in Enable mode.
- SSH—SSH username and password.
- SSH Enable Mode User Name and Password—SSH username and password in Enable mode.

To view all these credentials select **All**.

By default, these credentials are checked:

- SNMP Read Community String
- SNMP Write Community String
- Telnet
- Telnet Enable Mode User Name and Password

Step 3 Click **OK**.

To select the verify device credentials while adding devices:

Step 1 Select **Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**.

The Device Management Settings dialog box appears.

Step 2 Select **Verify Device Credentials While Adding Devices**.

Step 3 Click **OK**.

To view the device verification report:

Note Before performing the step 3, you must add devices to RME. See Adding Devices to RME to add devices to RME.

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Device Credential Verification Jobs**.

The Device Credential Verification dialog box appears.

Step 2 Select the devices that was added newly using either the RME@*ciscoworks_server* or CS@*ciscoworks_server* group.

Step 3 Schedule a job for the selected devices.

Using the RME Devices Window

This window lists all devices in RME. This window contains the following pane and buttons:

Table 3-1 RME Devices Window

Pane/Buttons	Description
RME Device Selector (Pane)	This lists all devices in RME. The devices are identified by the Display Name that you have entered while adding devices to Device and Credential Repository. See Using RME Device Selector for more information.
Add Devices (Button)	Add devices to RME manually. See Adding Devices to RME.
Edit Device Attributes (Button)	Editing the RME device attributes. The device attributes are: • Serial Number • SNMP Retry • SNMP Timeout • Telnet Timeout • Natted RME IP Address • TFTP Timeout See Editing RME Device Attributes.

Table 3-1 RME Devices Window (continued)

Pane/Buttons	Description
Delete (Button)	Delete RME devices. See Deleting Devices from RME.
Export (Button)	Export the RME device credentials into to a file. The supported export file formats are CSV (version 3.0 and XML). See Exporting RME Device Credentials.

Adding Devices to RME

You can either:

- Add devices manually (See Adding Devices to RME Manually)

Or

- Add devices automatically (See Adding Devices to RME Automatically)

Before adding devices to RME, you must add devices into Device and Credential Repository (**Common Services > Device and Credentials > Device Management**).

By default, the Automatically Manage Devices from Credential Repository option in the Device Management Settings window is enabled.

When you add devices to Device and Credential Repository and RME is down, the devices are added automatically when RME comes up again. The devices are added automatically, if the Automatically Manage Devices from Credential Repository option is enabled.

If this option is not enabled, you must manually add the devices.

Notes on Cluster Management Devices and Proxy Devices

The following is additional information on:

- Cluster Management Devices

  If you have added the DSBU Cluster Commander to DCR with the device type as Cisco Cluster Management Suite, it does not appear in the RME device selector. You must add this Commander in DCR, as Member. Normally, the Commander is 0^{th} member of the cluster.

  For more information, see the section Cluster Managed in the Adding Devices to the Device and Credential Repository Common Services Online help.

  Similar to other devices, these cluster members are managed in RME and you can perform all RME tasks on them.

- Proxy Devices

  All relationships between the Cisco Standard devices and Proxy Managers are considered while adding devices to DCR.

  The Proxy managed devices can be added to RME in the same way as other Cisco Standard devices. RME displays these Proxy managed devices in the same way as it displays other Cisco Standard Devices.

After adding devices to RME, RME automatically schedules for a device inventory and configuration collection.

For Inventory collection to happen, you must ensure that you have entered the correct read community string in Device and Credential Repository. RME acquires inventory data from devices using SNMP queries to both standard SNMP MIB II objects and Cisco-specific enterprise MIB objects.

For Configuration collection to happen, you should have entered the correct read and write community strings and telnet credentials in Device and Credential Repository.

See Supported Device Table for RME 4.0 on Cisco.com to know the list of devices that are supported in RME:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055bb65.html

Licensing Behavior While Adding Devices

If the number of devices that you added in Device and Credential Repository exceeds the licensed device limit, RME selects the option that results in fewer devices. The options are:

- The number of devices permitted by the license and an additional 10% of the licensed device limit are added.

  Or
- The number of devices permitted by the license and an additional 100 devices are added

For example, if you have a license for 5000 devices, you are allowed to manage only up to 5100 devices. This is because 10% of 5000 devices is 500 devices, which is more than 100 devices.

Licensing Behavior While Adding Devices Automatically

If you have enabled the Automatically Manage Devices from Credential Repository option and reached the maximum device limit, when you continue to add devices to Device and Credential, the option that results in fewer devices is selected and added to RME.

For example, if you have a license for 300 devices and you attempt to add 40 more devices, only 330 devices are added. The remaining 10 devices continue to be in Device and Credential Repository.

Licensing Behavior While Adding Devices Manually

If you have disabled the Automatically Manage Devices from Credential Repository option, reached the maximum device limit, and selected a large number devices for adding into RME, none of devices are added.

For example, if you have a license for 300 devices and attempt to add 40 more devices, none of these devices are added to RME.

Adding Devices to RME Manually

You can use this option to selectively add devices to RME from Device and Credential Repository or when you have deleted devices in RME and you want to readd those devices to RME.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To add devices to RME manually:

Step 1 Check if the *Automatically Manage Devices from Credential Repository* on Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt**) is disabled.

Step 2 Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

The RME Devices dialog box appears.

Step 3 Click **Add Devices** without selecting any devices from the RME Device Selector.

The Devices in Device Credential Repository dialog box appears.

If there are no devices in Device and Credential Repository that needs to be added in RME, a message appears, `There are no new devices in DCR. Please click here to add devices in DCR.`

If you want to add devices to Device and Credentials Repository, then click on the link or click **OK** to exit.

Step 4 Select the devices from the group.

- To select all the devices, select the All Devices check box.
- To select particular device type, select the Device Type Groups check box, and select the device type (for example, Routers, Switches and Hubs, etc.).
- To select devices from User Defined Groups, select the User-Defined Groups checkbox and expand the Common Services group till you see the device Display Name and then select the device.

To see the list of selected devices, click on the Selection tab. You can deselect the devices if you want.

You can also search for devices from the Device Selector. For more details, see Using RME Device Selector.

Step 5 Click **Next**.

The View RME Attributes dialog box appears with the following information:

Column Name	**Description**
Device Display Name	Display name of the device as entered in Device and Credential Repository.
Serial Number	Cisco manufacturing serial number from chassis. You can enter 0 to 255 alphanumeric characters. The default value is Default Not Defined.
SNMP Retry (Count)	Number of times, system should try to access devices with SNMP options. The default value is 2. The minimum value is zero.
SNMP Timeout (Secs)	Amount of time, system should wait for a device to respond before it tries to access it again. The default value is 2 seconds. The minimum value is zero seconds. There is no maximum value limit. Changing the SNMP timeout value affects inventory collection.

Column Name	Description
Telnet Timeout (Secs)	Amount of time, system should wait for a device to respond before it tries to access it again. The default value is 36 seconds. The minimum value is zero seconds. There is no maximum value limit. Changing the Telnet timeout value affects inventory collection.
Natted RME IP Address	The RME server ID. This is the translated address of RME server as seen from the network where the device resides. This is used when RME tries to contact devices outside the NAT boundary. The default value is Default Not Defined. See Managing Devices When RME Server is Within a NAT Boundary for further details.

Step 6 Click either

- **Export** to edit the RME device attributes in bulk.

  Or

- **Edit Device Attributes** to edit the RME device attributes for a single device.

  See Editing Device Attributes While Adding Devices to RME for more details.

Step 7 Click **Finish**.

A notification window displays, `Devices selected will be added to RME. Click on Pending Devices to verify the progress.`

Step 8 Click **OK**.

The RME Devices window appears with the newly added devices.

To view the RME device state, click on **Resource Manager Essentials > Devices > Device Management**.

Editing Device Attributes While Adding Devices to RME

In the View RME Attributes dialog box you can either click

- **Export** to edit the RME device attributes in bulk.

  Or

- **Edit Device Attributes** to edit the RME device attributes for a single device.

If you click on the Export button, then follow this procedure to edit the device attributes:

Step 1 Click **Export**.

The Export Device Credentials to File dialog box appears.

Step 2 Enter the folder name and the filename on the RME server.

Or

Click **Browse** to select a folder on the RME server.

The Server Side File Browser dialog box appears.

a. Select a folder and enter the filename on the RME server.

b. Click **OK**.

Step 3 Click **OK**.

Step 4 Edit the exported file.

You can edit only the RME device attributes, Serial Number, SNMP Retry, SNMP Timeout, Telnet Timeout, and Natted RME IP Address. You cannot edit the Device Display Name (device_identity) or add new device entries.

See RME Device Attributes Export File Format for further information.

Step 5 Click **Import**

The Import Device Credentials to File dialog box appears.

We recommend that you import the same file that you have exported after editing. If any new device entries are added, these device entries are ignored. Only device entries that match the existing device entries are imported.

Step 6 Enter the folder name and the filename on the RME server.

Or

Browse to select a folder on the RME server.

The Server Side File Browser dialog box appears.

a. Select a folder and file on the RME server.

b. Click **OK**.

Step 7 Click **OK**.

The RME Device Attributes window refreshes and displays the updated RME device attributes.

While importing the edited RME device attributes file an error message may appear,
`Attribute values for some selected devices are invalid. See Attribute Error Report for details.`

See Editing RME Device Attributes section to know the minimum and maximum values for the RME device attributes. Also see Attribute Error Report for more information.

See Adding Devices to RME Manually to continue to manually add devices to RME.

If you click on the Edit Device Attributes button, follow this procedure to edit the device attributes:

Step 1 Click **Edit Device Attributes**.

The Device Attributes Information dialog box appears.

Step 2 Select a device from the Devices pane, if you want to modify the attributes of that device.

Or

Select all devices by checking **Apply to All Devices** checkbox, if you want to apply the attributes of one device to all other devices that are listed in the Devices pane.

Step 3 Edit the device attributes in the Device Information pane.

Step 4 Click **Modify**.

See Adding Devices to RME Manually to continue the procedure of adding devices to RME manually.

Adding Devices to RME Automatically

Whenever you add devices to Common Services' Device and Credential Repository, RME triggers the Device Auto Management service. The devices that are added to Device and Credential Repository gets added to RME automatically.

By default, the Automatically Manage Devices from Credential Repository option in the Device Management Settings window is enabled.

The Device Auto Management service gets triggered when you add devices to Common Services' Device and Credential Repository through

- User interface (**Common Services > Device and Credentials > Device Management**).
- Command line tool `dcrcli`

This service is not triggered when you upgrade a RME license file.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To enable the Device Auto Management setting:

Step 1 Select **Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**.

The Device Management Settings dialog box appears.

Step 2 Select Automatically Manage Devices from Credential Repository.

Step 3 Click **OK**.

Here after, if any new devices are added in Device and Credential Repository (**Common Services** > **Device and Credentials** > **Device Management**) these devices get added into RME.

If there are any devices that are deleted from RME before enabling this option, those devices are not added to RME. You have to add those devices to RME manually. See Adding Devices to RME Manually.

Click either on

- **Resource Manager Essentials > Devices > Device Management** to view the RME device state.

  Or
- **Resource Manager Essentials > Devices > Device Management > RME Devices** to view the RME devices.

Editing RME Device Attributes

The RME device attributes are:

- Serial Number

  Cisco manufacturing serial number from chassis. You can enter alphanumeric characters up to 255.

The default value is Default Not Defined.

This attribute is available when you either export or edit the RME device attributes from the RME Devices window (**Devices > Device Management > RME Devices**).

- SNMP Retry

  Number of times that the system should try to access devices with SNMP options.

  The default value is 2. The minimum value is zero.

- SNMP Timeout

  Duration of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 2 seconds. The minimum value is zero seconds. There is no maximum value limit.

  Changing the SNMP timeout value affects inventory collection.

- Telnet Timeout

  Duration of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 36 seconds. The minimum value is zero seconds. There is no maximum value limit.

- Natted RME IP Address

  The RME server ID. This is the translated address of RME server as seen from the network where the device resides.

  This is used when RME tries to contact devices outside the NAT boundary and you need to enable support for NAT.

  The default value is Default Not Defined.

  See Managing Devices When RME Server is Within a NAT Boundary for further details.

- TFTP Timeout

  Duration of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 5 seconds and the minimum value is 0 seconds. There is no maximum value limit.

  This attribute is available only when you edit the RME device attributes from the RME Device Attributes window (**Admin > System Preferences > RME Device Attributes**).

Do any one of the following to set or edit the RME device attributes:

- Set the default device attributes value for all RME devices using **Resource Manager Essentials > Admin > System Preferences > RME Device Attributes**. See To set default device attributes
- Set the device attributes value for a single RME device using **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes** > **Inline Edit**. See To set or edit the RME device attributes for a single RME device
- Set the device attributes value for the bulk of RME devices using **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes > Export**. See To set or edit the RME device attributes for the bulk of RME devices

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To set default device attributes

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > RME Device Attributes**.

The RME Device Attributes dialog box appears.

Step 2 Enter the default value for:

- SNMP Retry
- SNMP Timeout
- Telnet Timeout
- Natted RME IP Address
- TFTP Timeout

The value you enter here will be applicable for all RME devices.

You can change the value for a single or bulk devices and also enter the device serial number information using the Edit Device Attributes option on RME Devices window. (see To set or edit the RME device attributes for a single RME device and To set or edit the RME device attributes for the bulk of RME devices.)

Step 3 Click **Apply**.

A confirmation message appears, `Default settings are updated successfully`.

Step 4 Click **OK**.

To set or edit the RME device attributes for a single RME device

---

Step 1 Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

The RME Devices dialog box appears.

Step 2 Select the devices for which you want to edit the RME device attributes. See Using RME Device Selector for further information.

Step 3 Click **Edit Device Attributes**.

The RME Device Attributes dialog box appears.

Step 4 Click **Inline Edit**.

The Device Attributes Information dialog box appears.

Step 5 Select a device from the Devices pane.

Step 6 Edit the device attributes in the Device Information pane.

You can check the **Apply to all Devices** checkbox to apply the device attributes of one device to all other devices that are listed in the Devices pane.

Step 7 Click **Modify** in the Device Attributes Information dialog box.

Step 8 Click **Apply** in the RME Device Attributes dialog box.

To set or edit the RME device attributes for the bulk of RME devices

---

Step 1 Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

The RME Devices dialog box appears.

Step 2 Select the devices for which you want to edit the RME device attributes. See Using RME Device Selector for further information.

Step 3 Click **Edit Device Attributes**.

The RME Device Attributes dialog box appears.

Step 4 Click **Export**.

The Export Device Attributes to File dialog box appears.

a. Enter the folder name and the filename on the RME server.

Or

- Browse to select a folder on the RME server.

  The Server Side File Browser dialog box appears.
- Select a folder and enter the filename on the RME server.
- Click **OK** in the Server Side File Browser dialog box.

b. Click **OK** in the Export Device Attributes to File dialog box.

The notification window displays `Data exported successfully`.

c. Click **OK** in the notification window.

Step 5 Edit the exported file.

You can edit only the RME device attributes, Serial Number, SNMP Retry, SNMP Timeout, Telnet Timeout, and Natted RME IP Address. You cannot edit the Device Display Name (device_identity) and add new device entries.

See RME Device Attributes Export File Format for further information.

Step 6 Click **Import** in the RME Device Attributes dialog box.

The Import Device Attributes to File dialog box appears.

We recommend that you import the same file that you have exported after editing. If any new device entries are added, these device entries are ignored. Only device entries that match the existing device entries are imported.

a. Enter the folder name and the filename on the RME server.

Or

- Browse to select a folder on the RME server.

  The Server Side File Browser dialog box appears.
- Select a folder and file on the RME server.
- Click **OK** in the Server Side File Browser dialog box.

b. Click **OK** in the Import Device Attributes to File dialog box.

The notification window displays `Data imported successfully`.

c. Click **OK** in the notification window.

The RME Device Attributes window refreshes to display the updated RME device attributes.

While importing the edited RME device attributes file an error message may appear, `Attribute values for some selected devices are invalid. See Attribute Error Report for details.`

See Editing RME Device Attributes section to know the minimum and maximum values for the RME device attributes. Also see Attribute Error Report for more information.

Step 7 Click **Apply**.

The RME Devices window appears.

Attribute Error Report

The Attribute Error report is generated when the attribute values imported for some selected devices are invalid. This error occurs when the device attributes that are imported as a CSV file contain invalid attributes.

You can click on the **Attribute Error Report** link which is displayed in the error message, to open the Attribute Error Report.

You can also view the Attribute Error Report by clicking on the **Attribute Error Report** button from the following locations:

- **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes**
- **Resource Manager Essentials > Devices > Device Management > RME Devices > Add Devices > Next**

Note The Attribute Error Report link is available only if importing of device attributes causes error.

RME Device Attributes Export File Format

The RME device attributes are exported in CSV 3.0 format. The exported file format is:

```
; This file is generated by DM Export utility

Cisco Systems NM Data import, Source=DM Export; Type=DMCSV; Version=3.0

;

;Start of section 0 - DM Export

;

;HEADER: device_identity,serial_number,SNMPRetryCount,SNMPTimeout,TelnetTimeout,RMEId

;

192.168.8.4,Default Not Defined,2,2,36,Default Not Defined

;End of CSV file
```

Where,

- `device_identity`–Display name of the device as entered in Device and Credential Repository.
- `serial_number`—Cisco manufacturing serial number from chassis. You can enter 0 to 255 alphanumeric characters. The default value is `Default Not Defined`.
- `SNMPRetryCount`—Number of times, system should try to access devices with SNMP options. The default value is 2. The minimum value is zero.
- `SNMPTimeout`—Duration of time the system should wait for a device to respond before it tries to access it again. The default value is 2 seconds. The minimum value is zero seconds. There is no maximum value limit.

Changing the SNMP timeout value affects inventory collection.

- `TelnetTimeout`—Duration of time the system should wait for a device to respond before it tries to access it again. The default value is 36 seconds. The minimum value is zero seconds. There is no maximum value limit.
- `Natted RME IP Address`—RME server ID. This is the translated address of RME server as seen from the network where the device resides. This is used when RME tries to contact devices outside the NAT boundary. The default value is `Default Not Defined`.

Exporting RME Device Credentials

You can export the device credentials for the RME devices in CSV or XML format.

You can also export RME device credentials using the command line tool, **`cwcli inventory crmexport`**. See Overview: cwcli inventory Command.

You can import the edited device credentials using **Common Services > Device and Credentials > Device Management > Bulk Import**.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To export RME devices credentials:

Step 1 Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

The RME devices dialog box appears.

Step 2 Select the RME devices. See Using RME Device Selector for further information.

Step 3 Click **Export**.

A message appears, `Export will store password in clear text. Do you still want to continue?`

Step 4 Click **OK** to continue or **Cancel** to abort the export.

If you click **OK**, then the Export To File dialog box appears.

a. Enter the folder name and the filename on the RME server.

Or

  - Browse to select a folder on the RME server.

    The Server Side File Browser dialog box appears.

  - Select a folder and file on the RME server.
  - Click **OK**.

b. Select the file format, CSV or XML.

The supported version for CSV is 3.0.

Warning **The device passwords will be displayed in plain text.**

Step 5 Click **OK**.

The RME devices dialog box appears.

The exported file is saved on the RME server.

You can import the edited device credentials using **Common Services > Device and Credentials > Device Management > Bulk Import**.

See Common Services Online help for further information on export file formats and procedure for importing a device file.

Deleting Devices from RME

The devices in the Delete state cannot participate in any RME application flows. The Delete devices historical data is not retained in the RME database.

However, you can re-add the devices using **Resource Manager Essentials > Devices > Device Management > RME Devices** > **Add Devices**.

The device information is retained in the Device and Credential Repository. This information is not removed till you delete the device from **Common Services > Device and Credentials > Device Management**.

If RME is down when you delete devices from Device and Credential Repository, the devices get deleted from RME when RME is back online.

You can also delete the RME devices using the command line tool, **`cwcli inventory deletedevice`**. See Overview: cwcli inventory Command.

For NAM devices, the Supervisor device must be in RME. You cannot work with NAM devices if the Supervisor device is not in RME.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To delete devices from RME:

Step 1 Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

The RME devices dialog box appears.

Step 2 Select the RME devices. See Using RME Device Selector for further information.

A message appears, `Are you sure you want to delete?`

Step 3 Click **OK**.

The RME Devices window appears without the deleted device.

You can view the Deleted devices by navigating to **Resource Manager Essentials** > **Devices** > **Device Management** > **RME Devices > Add Devices** as these devices still exist in Device and Credential Repository.

Understanding the RME Device States

After adding devices in RME, you can check the state of the RME devices using **Resource Manager Essentials** > **Devices** > **Device Management** option.

You can also view the RME devices state using the command line tool **`cwcli inventory getdevicestate`**. See Overview: cwcli inventory Command.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Refresh Icon	Click on this icon to refresh the RME device states.

The RME devices can be in one of the following states:

Normal

In the Normal device state, the device has been successfully contacted by RME or the device has contacted RME at least once (polling, successful job completion, Syslog receipt etc.). This indicates that this is a real device in the network (at one point in time).

This state does not guarantee that we have had a successful Inventory and Configuration Collection.

See Working With Normal Devices for further details on Normal devices.

Pre-deployed

In the Pre-deployed device state, the device has never been contacted by RME through protocols such as SNMP, Telnet, SSH, etc. If RME successfully contacts the device through the tasks such as Inventory polling, Configuration polling receiving syslog messages, etc., the device will move to a Normal state.

The Pre-deployed device state, indicates that the devices are not in the network and are awaiting to be deployed.

See Working With Pre-deployed Devices for further details on Pre-deployed devices.

Alias

When you add a new device to RME, this device may already exist in RME, but with another hostname or IP address. This device will be in the Alias state.

See Working With Alias Devices for further details on Alias devices.

Pending

When the device is added to RME, RME device management moves the device into this state, and invokes all the registered application tasks such as Inventory Collection and Configuration collection.

Based on the results of the tasks, the device moves to one of these states—Pre-deployed, Normal or Aliased.

The Pending state is a transient state and no device will be in this state for any significant time.

See Working With Pending Devices for further details on Pending devices.

Conflicting

The Conflicting device state occurs if the sysObjectID in the device and that in the Device and Credential Repository do not match.

See Working With Conflicting Device Types for further details on Conflicting devices.

Suspended

Sta te of a device by virtue of explicit action wherein a device cannot participate in any application flows but all historical data pertaining to the device will continue to be maintained by RME. You can re-submit the devices in this state for participation in RME workflows.

See Working With Suspended Devices for further details on Suspending devices.

See Understanding RME Device State Transition to understand the RME device state transitions.

Working With Normal Devices

In the Normal device state, the device has been successfully contacted by RME or the device has contacted RME at least once (polling, successful job completion, Syslog receipt etc.). This indicates that this is a real device in the network (at one point in time).

This state does not guarantee that you have had a successful Inventory and Configuration Collection.

You can schedule for a Inventory Collection using **Resource Manager Essentials > Devices > Inventory > Inventory Jobs** (Create button) and Configuration Collection using **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive**.

You can perform all the RME application tasks using RME Normal device state.

The Normal Devices window (Table 3-2*)* contains the following pane and buttons:

Table 3-2 Normal Devices Window

Pane/Buttons	Description
RME Device Selector (Pane)	This lists all devices in RME. The devices are identified by the Display Name that you have entered while adding devices to Device and Credential Repository. See Using RME Device Selector for more information.
Export (Button)	Export the Normal state devices. See Exporting the Normal Devices Credentials
Suspend (Button)	Suspend the Normal state devices. See Suspending the Normal Devices
Delete (Button)	Delete the Normal state devices. See Deleting the Normal Devices
Resubmit (Button)	Resubmit the Normal state devices. See Resubmitting the Normal Devices
Refresh (Icon)	Click on this icon to refresh the RME device states.

Exporting the Normal Devices Credentials

To export the Normal device list:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Normal Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Normal Device State.

The Normal devices dialog box appears.

Step 2 Select the RME devices that are in Normal state. See Using RME Device Selector for more information.

Step 3 Click **Export**.

A message appears, `Export will store password in cleartext. Do you still want to continue?`

Step 4 Click **OK** to continue or **Cancel** to abort the export.

If you click **OK**, then the Export To File dialog box appears.

Step 5 Enter the folder name with the file name on the RME server.

Or

Browse to select a folder on the RME server.

The Server Side File Browser dialog box appears.

- **a.** Select a folder on the RME server.
- **b.** Click **OK**.
- **c.** Enter the file name with the file extension either CSV or XML.

Step 6 Select the Export File Type, CSV or XML.

The supported version for CSV is 3.0.

Warning **The device passwords will be displayed in plain text.**

Step 7 Click **OK**.

The devices that you have selected will be exported.

See Common Services Online help for further information on export file formats.

Suspending the Normal Devices

The devices in the Suspended state cannot participate in any RME application flows. However, you can re-submit the devices in this state for participation in RME workflows using **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**. The Suspend devices historical data is retained in the RME database.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To suspend the Normal device list:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Normal Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Normal Device State.

The Normal devices dialog box appears.

Step 2 Select the RME devices that are in Normal state. See Using RME Device Selector for more information.

Step 3 Click **Suspend**.

A confirmation dialog box appears.

Step 4 Click **OK**.

You can view the Suspended device list by navigating to **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Deleting the Normal Devices

The devices in the Delete state cannot participate in any RME application flows. The Delete devices historical data is not retained in the RME database. However, you can re-add the devices using **Resource Manager Essentials > Devices > Device Management > Add Devices**.

The device information is retained in the Device and Credential Repository. This information is not removed till you delete the device from **Common Services > Device and Credentials > Device Management**.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To delete the Normal devices:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Normal Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Normal Device State.

The Normal devices dialog box appears.

Step 2 Select the RME devices that are in Normal state. See Using RME Device Selector for more information.

Step 3 Click **Delete**.

A confirmation dialog box appears.

Step 4 Click **OK**.

You can view the Deleted devices by navigating to **Resource Manager Essentials** > **Devices** > **Device Management** > **Add devices** as these devices still exist in Device and Credential Repository.

Resubmitting the Normal Devices

Whenever you change any of the device credentials in the Device and Credential Repository using **Common Services > Device and Credentials > Device Management**, the RME may not get updated.

For example, if you perform any one of the following updates in the Device and Credential Repository, you must also update the RME. Otherwise some of the RME tasks may fail:

- If you update sysObjectID, Device type, or MDF type in the Device and Credential Repository incorrectly, RME may not change the Normal device state to Conflicting device state. So RME applications that access the Device and Credential Repository may fail.
- If you update the IP address or hostname in the Device and Credential Repository, RME may not trigger inventory collection.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To update the RME whenever there is change in the Device and Credential Repository:

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Normal Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Normal Device State.

The Normal Devices dialog box appears.

Step 2 Select the RME devices that are in Normal state. See Using RME Device Selector for more information.

Step 3 Click **Resubmit**.

A confirmation dialog box shows that the devices has been added to the Pending list.

Step 4 Click **OK**.

The devices are re-added to the RME.

To view the device status, click **Resource Manager Essentials > Devices > Device Management**.

Generating the Inventory and Configuration Collection Status Report

You can view the status of the last Inventory and Configuration collection.

If the collection status is failed, you can schedule for a Inventory Collection using **Resource Manager Essentials > Devices > Inventory > Inventory Jobs** (Create button) and Configuration Collection using **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive**.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate a collection status report:

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Normal Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Normal Device State.

The Normal Devices dialog box appears.

Step 2 Select the RME devices that are in Normal state. See Using RME Device Selector for more information.

Step 3 Click **Report**.

The Device Status Report appears in a separate browser window.

See Checking Configuration Archival Status to understand the different configuration collection status.

The following buttons are available on the Device Status Report:

Button	Description
Export to File (Icon)	You can export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Working With Pending Devices

When the device is added to RME, RME device management moves the device into this state, and invokes all the registered application tasks such as Inventory Collection and Configuration collection.

Based on the results of the tasks, the device moves to one of these states—Pre-deployed, Normal or Aliased.

The Pending state is a transient state and no device will be in this state for any significant time. If the devices are in this state for a longer time, you can suspend the devices and resubmit for managing.

To do this use, **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

The Pending Devices window (Table 3-3)contains the following pane and button:

Table 3-3 Pending Devices Window

Pane/Buttons	Description
Device Identity (Pane)	This lists all devices in RME that are in Pending state. The devices are identified by the Display Name that you have entered while adding devices to Device and Credential Repository.
Suspend (Button)	Suspend the Pending state devices. See To suspend the Pending devices: This button gets activated only after selecting devices from Device Identity pane.
Refresh (Icon)	Click on this icon to refresh the RME device states.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To suspend the Pending devices:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Pending Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Pending Device State.

The Pending devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Suspend**.

A confirmation dialog box appears.

Step 4 Click **OK**.

You can view the Suspended device list by navigating to **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Working With Suspended Devices

Suspended device state cannot participate in any RME application flows but all historical data pertaining to the device will continue to be maintained by RME.

The Suspended Devices window (Table 3-4)contains the following pane and buttons:

Table 3-4 Suspended Devices Window

Pane/Buttons	Description
Device Identity (Pane)	This lists all devices in RME that are in Suspended state. The devices are identified by the Display Name that you have entered while adding devices to Device and Credential Repository.
Resubmit (Button)	Re-submit the Suspended state devices. See Resubmitting the Suspended Devices. This button gets activated only after selecting devices from Device Identity pane.
Delete (Button)	Delete the Suspended state devices. See Deleting the Suspended Devices. This button gets activated only after selecting devices from Device Identity pane.

Resubmitting the Suspended Devices

If you want to re-add the devices to RME, then you can re-submit the Suspended devices:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To re-submit the Suspended devices:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Suspended Device State.

The Suspended devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Resubmit**.

A confirmation dialog box appears.

Step 4 Click **OK**.

You can view the state of these RME devices using **Resource Manager Essentials** > **Devices** > **Device Management**.

Deleting the Suspended Devices

The devices in the Delete state cannot participate in any RME application flows. The Delete devices historical data is not retained in the RME database. However, you can re-add the devices using **Resource Manager Essentials > Devices > Device Management > Add Devices**.

The device information is retained in the Device and Credential Repository. This information is not removed till you delete the device from **Common Services > Device and Credentials > Device Management**.

To delete the Suspended devices:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Suspended Device State.

The Suspended devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Delete**.

A confirmation dialog box appears.

Step 4 Click **OK**.

You can view the Deleted devices by navigating to **Resource Manager Essentials** > **Devices** > **Device Management** > **Add devices** since these devices still exist in Device and Credential Repository.

Working With Pre-deployed Devices

In the Pre-deployed device state, the device has never been contacted by RME through protocols such as SNMP, Telnet, SSH, etc. If RME successfully contacts the device through the tasks such as Inventory polling, Configuration polling receiving syslog messages, etc., the device will move to a Normal state.

In the Pre-deployed device state, there is no successful inventory or configuration collection for the device.

The Pre-deployed device state indicates that the devices are not in the network and are waiting to be deployed.

The Pre-deployed devices appear in the RME device selector as a separate group. These devices also appear under the appropriate MDF-based groups, depending on the Device Type information that you have entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management**).

You can perform application tasks (including jobs) on Pre-deployed devices in the same way as you do with the Normal state devices.

However, for Pre-deployed devices you cannot run application tasks such as Distribution By devices [Basic] job, Distribution By image job, etc. This is because the information needed for such tasks will be available only after RME contacts the devices.

For example, Software Management Distribution By devices [Advanced] job succeeds. This is because no data (either current or cached) is needed from the device for this task.

However, Software Management Distribution By devices [Basic] job fails. This is because the device inventory data is needed from the device for this task.

For all devices in the pre-deployed state, you can schedule:

- The RME Inventory polling and collection jobs (**Resource Manager Essentials > Devices > Inventory > Inventory Jobs**)
- The RME Configuration polling and collection jobs (**Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive**).

If RME succeeds in contacting the device for any of these jobs, the device will be moved to the Normal state.

See Understanding RME Device State Transition to understand the RME device state transition.

The Pre-Deployed Devices window (Table 3-5) contains the following pane and buttons:

Table 3-5 Pre-Deployed Devices Window

Pane/Buttons	Description
Device Identity (Pane)	This lists all devices in RME that are in Pre-deployed state. The devices are identified by the Display Name that you have entered while adding devices to Device and Credential Repository.
Export (Button)	Export the Pre-deployed state devices. See Exporting the Pre-deployed Device Credentials.
Suspend (Button)	Suspend the Pre-deployed state devices See Suspending the Pre-deployed Devices.
Resubmit (Button)	Re-submit the Pre-deployed state devices. See Resubmitting the Pre-deployed Devices. This button gets activated only after selecting devices from Device Identity pane.
Delete (Button)	Delete the Pre-deployed state devices. See Deleting the Pre-deployed Devices. This button gets activated only after selecting devices from Device Identity pane.
Refresh (Icon)	Click on this icon to refresh the RME device states.

See Diagnosing Pre-deployed Devices section to understand the probable cause for the device to be in Pre-deployed state and what action that needs to be taken to move the device to the Normal state.

Exporting the Pre-deployed Device Credentials

To export the Pre-deployed device list:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Pre-Deployed Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Pre-deployed State.

The Pre-Deployed Devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Export**.

A message appears, `Export will store password in cleartext. Do you still want to continue?`

Step 4 Click **OK** to continue or **Cancel** to abort the export.

If you click **OK**, then the Export To File dialog box appears.

Step 5 Enter the folder name with the file name on the RME server.

Or

Browse to select a folder on the RME server.

The Server Side File Browser dialog box appears.

a. Select a folder on the RME server.
b. Click **OK**.
c. Enter the file name with the file extension either CSV or XML.

Step 6 Select the Export File Type, CSV or XML.

Warning **The device passwords will be displayed in plain text.**

Step 7 Click **OK**.

The devices that you have selected will be exported.

See Common Services Online help for further information on export file formats.

Suspending the Pre-deployed Devices

The devices in the Suspended state cannot participate in any RME application flows. However, you can re-submit the devices in this state for participation in RME workflows using **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To suspend the Pre-deployed device list:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Pre-Deployed Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the **Pre-Deployed** State.

The Pre-Deployed Devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Suspend**.

A confirmation dialog box appears.

Step 4 Click **OK**.

To view the Suspended device list navigate to **Resource Manager Essentials** > **Devices** > **Device Management** > **Suspended Devices**.

Deleting the Pre-deployed Devices

The devices in the Delete state cannot participate in any RME application flows. The Delete devices historical data is not retained in the RME database. However, you can re-add the devices using **Resource Manager Essentials > Devices > Device Management > Add Devices**.

The device information is retained in the Device and Credential Repository. This information is not removed till you delete the device from **Common Services > Device and Credentials > Device Management**.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To delete the Pre-deployed devices:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Pre-Deployed Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Pre-deployed Device State.

The Pre-Deployed Devices dialog box appears.

Step 2 Select the devices.

Step 3 Click **Delete**.

A confirmation dialog box appears.

Step 4 Click **OK**.

To view the Deleted devices navigate to **Resource Manager Essentials** > **Devices** > **Device Management** > **Add devices** since these devices still exist in Device and Credential Repository.

Resubmitting the Pre-deployed Devices

Whenever you change any of the device credentials in the Device and Credential Repository using **Common Services > Device and Credentials > Device Management**, the RME may not get updated.

For example, if you perform any one of the following updates in the Device and Credential Repository, you must also update the RME. Otherwise some of the RME tasks may fail, for example if you update the IP address or hostname in the Device and Credential Repository, RME may not trigger inventory collection.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To update the RME whenever there is change in the Device and Credential Repository:

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Pre-Deployed Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Pre-deployed State.

The Pre-Deployed Devices dialog box appears.

Step 2 Select those devices where the credentials are updated in Device and Credential Repository using **Common Services > Device and Credentials > Device Management**.

Step 3 Click **Resubmit**.

A confirmation dialog box displays that the devices has been added to the Pending list.

Step 4 Click **OK**.

The devices will be re-added to the RME.

To view the device status, click **Resource Manager Essentials > Devices > Device Management**.

Diagnosing Pre-deployed Devices

This procedure can help you diagnose Pre-deployed devices which are displayed in the Device Management State Summary window.

You can follow any one of these methods to diagnose a Pre-deployed devices:

- Check if the inventory or configuration collection was successful. (See Procedure 1.)
- Check if the device credentials entered are correct. (See Procedure 2.)
- Check device connectivity by protocol, run ping on a device, and trace the route between the management station and a device. (See Procedure 3.)

Procedure 1

Check if the inventory or configuration collection was successful.

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Normal Devices**.

The Normal Devices dialog box appears.

Step 2 Select **Pre-deployed** devices group from RME@*CiscoWorksServer* device group.

Step 3 Click **Report**.

The Device Status Report appears in a separate browser window.

If the inventory or configuration collection has failed, you can schedule for a:

- Inventory collection using **Resource Manager Essentials > Devices > Inventory > Inventory Jobs > Create** (button).
- Configuration collection using **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive**.

Procedure 2

Check if the device credentials entered are correct.

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Device Credential Verification**.

The Device Credential Verification dialog box appears.

Step 2 Select **Pre-deployed** devices group from RME@*CiscoWorksServer* device group.

Step 3 Click **Check Device Credential**.

The Device Credentials Options dialog box appears.

Step 4 Select the device credentials that you want to verify and click **OK**.

A notification window appears, `Please Click on View Credential Verification Report Button to View the Report.`

Step 5 Click **OK**.

Step 6 Click **View Credential Verification Report**.

The Credential Verification Report appears.

To understand the reasons for failure click on the Failed link.

If the device credentials entered is incorrect, you can edit the credentials using **Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Edit Device Credentials**.

Procedure 3

Check device connectivity by protocol, run ping on a device, and trace the route between the management station and a device.

Step 1 Ping the device.

- If you specified the Pre-deployed device by IP address, ping to the IP address.
- Otherwise, send the request to the fully qualified host name.

Use the default settings for packet size, packet count, and timeout interval. If the ping succeeds, the device is on line and reachable, go to step 2.

If the ping fails because the:

- Device is an unknown host. The name service could not resolve the specified host name into an IP address.
- Device is unreachable. Your local system is unable to determine a route to the device.
- Device is not responding. Your local system was able to determine a route to the device, but the ping did not receive any responses to the ICMP echo-request packets it sent to the device.

Step 2 Open a Telnet session to the device to check its SNMP configuration.

If the device is not responding to the SNMP Get request packets from your server, make sure it has an SNMP agent that is enabled and accessible using the community strings you specified.

Use etherfind or another packet analyzer to investigate the SNMP packet exchange between your server and the SNMP agent on the device.

If the device does not support RFC 1213 (SNMP MIB II) attributes, it cannot be managed by RME.

Step 3 After you have corrected your device specification, your network connectivity, or both, resubmit the device.

If you try to re-import a device without modifying its device credentials using **Common Services > Device and Credentials > Device Management**, that device is not processed. Instead it is shown as a duplicate device in the Device Import Status window.

You should resubmit the Pre-deployed device using **RME > Devices > Device Management > Pre-deployed Devices > Resubmit** (button).

These tables describe the probable cause and the suggested action that needs to be taken when the devices are in Pre-deployed state:

- PingUtility Determines That the Device is an Unknown Host (Table 3-6)
- Ping Utility Determines That the Device in Unreachable (Table 3-7)
- Device Does not Respond to an ICMPEcho Request Packet (Table 3-8)
- Device Does not Respond to an SNMP Get Request Packet (Table 3-9)
- Device Does not Support RFC 1213(SNMP MIB II) Attributes (Table 3-10)

The following table describes what to do if the Ping utility determines that the device is an unknown host:

Table 3-6 Ping Utility Determines that the Device is an Unknown Host

Probable Cause	Suggested Action
Device hostname and/or domain name entered incorrectly.	Verify hostname and domain name in device integration source are spelled correctly. Make necessary corrections and resubmit the device using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button).
Name lookup registry does not contain entry for device.	If device hostname and domain name are correct and you know IP address, use ping to contact the device using the IP address. If the ping command is successful, the problem is with the name registry. 1. Use NSLookup to confirm the device name and server information. 2. Update the name registry to include the device by editing /etc/hosts file (on UNIX) or updating DNS or NIS servers. 3. Try the ping command again or add or import device using only the IP address. You can launch NSLookup using CiscoWorks LMS Portal home page > Device Troubleshooting > Device Center.

The following table describes what to do if the Ping utility determines that devices as unreachable:

Table 3-7 Ping Utility Determines That the Device is Unreachable

Probable Cause	Suggested Action
Device IP address entered incorrectly.	If you used IP address to specify device and the ping command failed in step 1, use the pingcommand to contact to device using its fully qualified hostname. If the ping command is successful, the problem is that the device IP address was added incorrectly in the device integration source. Correct the IP address.

The following table describes what to do if the device does not respond to an ICMP Echo request packet:

Table 3-8 Device Does not Respond to an ICMP Echo Request Packet

Probable Cause	Suggested Action
An intermediate device is powered down.	Determine which device is down and get this device back online. Use connectivity tools to find the source of the problem. You can launch connectivity tools using CiscoWorks LMS Portal home page > Device Troubleshooting > Device Center.
Device is powered down or administratively disabled.	Get the device back online.
Interface at polling destination (identified by IP address in DNS, and host and domain names) is broken or administratively disabled.	Verify interface is enabled and functioning properly.

Table 3-8 Device Does not Respond to an ICMP Echo Request Packet (continued)

Probable Cause	Suggested Action
The device or the intermediate network is busy.	Resubmit the device at a time when the device or network is less busy. You can resubmit using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button).
The interface at the polling destination is rebooting.	Resubmit the device later. You can resubmit using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button).
The connection path from the network management station to the device is a slow link.	Resubmit the device when network traffic is lighter. A heavy network load can cause packets to be dropped. You can resubmit using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button).
A section of the connection path from the network management station to the device is busy.	Resubmit the device when the segment is less busy. Use the connectivity tools to find the source of the problem. You can resubmit using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button). You can launch connectivity tools using CiscoWorks LMS Portal Home page > Device Troubleshooting > Device Center.
A section of the connection path from the network management station to the device is noisy and losing packets.	Check your ping statistics for excessive packet loss along the path. Resubmit the device when there is less traffic on the link. Use the connectivity tools to find the source of the problem. You can resubmit using RME > Devices > Device Management > Pre-deployed Devices > Resubmit (button). You can launch connectivity tools using CiscoWorks LMS Portal Home page > Device Troubleshooting > Device Center.
Ping is not enabled for that device.	Verify that ping is enabled on the device.
Ping is blocked by an intermediate device.	Verify that ping is enabled on the routers on the path to the device. Use the connectivity tools to find the source of the problem. You can launch connectivity tools using CiscoWorks LMS Portal home page > Device Troubleshooting > Device Center.

The following table describes what to do if the device does not respond to an SNMP Get request packet:

Table 3-9 Device Does not Respond to an SNMP Get Request Packet

Probable Cause	Suggested Action
The device does not have an SNMP agent.	None; RME manages only devices with SNMP MIB II agents.
The SNMP agent is not enabled on the device.	Verify that the SNMP agent is enabled.

Table 3-9 Device Does not Respond to an SNMP Get Request Packet (continued)

Probable Cause	Suggested Action
You entered the wrong SNMP community string.	Verify that you entered the SNMP Read and Write community strings correctly. You can verify the credentials using • Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Check Device Credential • Resource Manager Essentials > Devices > Device Management > Device Credential Verification > View Credential Verification Report You can edit the credentials using Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Edit Device Credentials.
Increase the SNMP timeout for that device	Increase the SNMP timeout for that device by exporting the device attributes using Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes (button).
An intermediate device is misconfigured and blocking the request.	Determine which device is blocking the request (routers are sometimes configured to block SNMP packets) and reconfigure the device. Use the connectivity tools to find the source of the problem. You can launch connectivity tools using CiscoWorks LMS Portal home page > Device Troubleshooting > Device Center.
Access Control Lists (ACLs) on the managed device prevent SNMP packets from reaching the SNMP agent.	Check the ACLs on the managed device (and possibly intermediary devices) to make sure that SNMP traffic gets to and returns from the agent. Use the connectivity tools to find the source of the problem. Reconfigure the ACLs on the problem devices to allow SNMP traffic. You can launch connectivity tools using CiscoWorks LMS Portal home page > Device Troubleshooting > Device Center.

The following table describes what to do if the device does not support RFC 1213 (SNMP MIB II) attributes:

Table 3-10 Device Does not Support RFC 1213 (SNMP MIB II) Attributes

Probable Cause	Suggested Action
The device has an old (RFC 1156) SNMP MIB I agent.	Upgrade the agent to RFC 1213 standards for SNMP MIB II.

Working With Alias Devices

When you add a new device to RME, this device may already exist in RME, but with another hostname or IP address. This device will be in the Alias state.

Detecting an Alias Device

The prerequisites for detecting an alias device are:

- The alias device is detected when you perform the first inventory collection for a device.
- A device is detected as an alias device only after a successful inventory collection. If a device is detected as an alias of another device, then that device is moved to an aliased state.

- For all devices already in aliased state, the RME reruns the alias detection algorithm again. This detection is performed whenever the inventory is collected successfully.

  This is done to ensure that the devices are still alias. If any of the devices are found to be not in an alias state, then RME moves these devices to Normal Device state.

  For example, this can happen after you correct the IP address of the device.
- If the inventory collection is partially successful or failed, an alias device may be listed as a Normal Device or as a Pre-deployed Device, based on whether the device was reachable or not.
- Devices in an alias state continue in the workflows as in their previous states (Normal/Pre-deployed/Pending).

You can resolve the alias by selecting one of the devices using **Resource Manager Essentials** > **Devices** > **Device Management** > **Alias Devices** (see Resolving an Alias Device). After you resolve the alias, all the rejected devices are deleted from the RME database.

Alias Detection Algorithm

RME detects an alias device using this algorithm. It:

1. Gets the device IP address, sysObjectID and the MAC address corresponding to the IP address of the new device.
2. Refers to the RME database for devices with same sysObjectID.
3. Refers to the RME database on devices returned in step 2 for IPaddresses and MAC addresses that match the addresses of the new device.
4. Compares the port count for the devices that match the criteria described in Step 2 and 3.
5. Identifies the new device as not being an alias device if no device is returned in step 4. Otherwise it identifies the new device as an alias device if the device is returned in step 4.

Resolving an Alias Device

To resolve an Alias device:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Alias Devices**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Alias Device State.

The Resolve Alias Devices dialog box appears. This dialog box contains two panes,

- Normal Devices—Lists the Normal devices that have aliases to the devices.
- Alias Devices—Lists the devices that are aliased to the Normal devices.

Step 2 Select a device from the Normal Devices pane to view the list of aliased devices.

Step 3 Click **Show Alias Devices**.

The devices that are aliased to the Normal devices appear in the Alias Devices pane. The devices that are in the Normal device state are also be listed along with the other alias devices.

Step 4 Select a device you want to resolve from the Alias Devices pane.

While resolving the alias state devices:

- If you have chosen to delete the device in the Alias Device state, all Syslog messages collected are retained.
- If you have chosen to delete the device in the Normal Device state, all Syslog messages collected are deleted.

We recommend that you delete the device in the Alias Device state and keep the device in the Normal Device state to retain all Syslog messages.

Step 5 Click **Select**.

The selected device is moved to either the Normal device state or the Pre-deployed device state, based on whether the device is reachable or not.

You can view the RME Device State using **Resource Manager Essentials** > **Devices** > **Device Management**.

Working With Conflicting Device Types

The Conflicting device state occurs if the sysObjectID in the device and that in the Device and Credential Repository do not match.

Detecting a Conflicting Device Type

The prerequisites for detecting an conflicting device are:

- The conflicting device is detected when you perform the first inventory collection for a device.
- A device is detected as an conflict device only after a successful inventory collection.
- If the inventory collection is partially successful or failed, a conflict device may be listed as a Normal Device or as a Pre-deployed Device, based on whether the device was reachable or not.
- Devices in Conflicting Device state cannot be included in the RME workflows. You must update the Device and Credential Repository with the correct device type so that these devices can be included in the RME workflows.

The devices go into Conflicting Device state because the device type that you entered in the Device and Credential Repository may be different from the device type that RME determines during inventory collection.

In such a case, RME Device Management provides a User Interface listing the devices with the incorrect device types. It also allows you to update the device type in the Device and Credential Repository or delete the device and re-submit the device for management.

Conflicting Device Type Algorithm

RME detects an conflict device using this algorithm:

1. RME gets sysObjectID from Device and Credential Repository.

   If the sysObjectID is null, RME updates the sysObjectID collected by Inventory collection, else go to step 2.

2. RME compares the sysObjectID in the Device and Credential Repository with the sysObjectID collected by Inventory application for a given device.

If they match, the device is moved to either Normal/Pre-deployed/Pending state. Otherwise, RME moves the device state to Conflict and allows you to update the Device and Credential Repository and resubmit the device for management or delete the device.

The Conflicting Device Types window contains the following fields and buttons:

Fields/Buttons	**Description**
Device Identity (Field)	This lists all Conflicting devices in RME. The devices are identified by the Display Name that you entered while adding devices to Device and Credential Repository.
SysObjectID in DCR (Field)	Displays sysObjectID that you have selected while adding devices to Device and Credential Repository.
SysObjectID found by RME (Field)	Displays sysObjectID that was found during RME Inventory Collection.
Update Credential Repository (Button)	Update the Device Credential Repository with the sysObjectID found by the RME. See Resolving the Conflicting Device Type. This button gets activated only after selecting devices from Device Identity pane.
Delete (Button)	Delete the Conflicting type devices. See Deleting the Conflicting Device Type. This button gets activated only after selecting devices from Device Identity pane.

Resolving the Conflicting Device Type

To resolve a Conflicting Device Type:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Conflicting Device Types**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Conflicting device state.

The Conflicting Device Types dialog box appears.

Step 2 Select a device.

Step 3 Click **Update Credential Repository**.

The conflicting device is moved to Normal device state.

You can view the RME Device State using **Resource Manager Essentials** > **Devices** > **Device Management**.

Deleting the Conflicting Device Type

To delete the Conflicting Device Type:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Devices** > **Device Management** > **Conflicting Device Types**.

Or

Select **Resource Manager Essentials** > **Devices** > **Device Management** and click on the Number of Device column entry for the Conflicting device state.

The Conflicting Device Types dialog box appears.

Step 2 Select a device.

Step 3 Click **Delete**.

A confirmation box appears.

Step 4 Click **OK**.

You can add the deleted devices to RME using **Resource Manager Essentials > Devices > Device Management > Add Devices**.

Checking and Viewing Device Credentials

You can check your device credentials for RME devices and view the results in a report. Use this option to make sure that your Device and Credential Repository credentials match your actual device credentials.

You can check the following device credentials:

- SNMP Read Community String—SNMP version 2 read community string.
- SNMP Write Community String—SNMP version 2 write community string.
- SNMPv3—SNMP version 3 username and password.
- Telnet—Telnet username and password.
- Telnet Enable Mode User Name and Password—Telnet username and password in Enable mode.
- SSH—SSH username and password.
- SSH Enable Mode User Name and Password—SSH username and password in Enable mode.

You can check the **All** checkbox to verify all the device credentials.

Click **Update** to save your settings or click **Reset** to discard the changes.

You can also verify the RME device credentials in two other ways:

- Using the command line tool, **`cwcli inventory cda`**.

  See Overview: cwcli inventory Command for further details.

- Using the Device Center (From CiscoWorks LMS Portal home page, Device Troubleshooting > Device Center to launch Device Center).

  See RME Device Center for further details.

Check Device Credentials Algorithm

Device Credential Verification verifies credentials that are device packages specific to a device type. These device packages may have variations in CLI access and respond to different transport protocols.

Device credential verification uses the credentials stored in Device and Credential Repository and validates these credentials against the corresponding device.

The following is the algorithm used to verify credentials for the device transport protocol:

- Read Community String

  Read community string is verified by performing read operation via the SNMP transport library and checking the result.

- Read/Write Community String

  a. Read write community string is verified by performing snmpget operation on syslocation variable.

  b. snmpset is performed with the value returned in the previous step.

  If the error message returned is,

  - *snmpRspBadValue* then the Read/Write community string is considered correct.
  - *snmpRspNoSuchName* then the Read/Write community string is considered wrong.

- Telnet Username and Password

  Telnet username and password are verified by trying to login to the device using the Telnet transport library. It also verifies if the attempt is successful.

- SSH Username and Password

  SSH username and password are verified by trying to login to the device using the SSH transport library. It also verifies if the attempt is successful.

- Telnet enable mode password

  Enable mode password is verified while trying to establish connection using Telnet and entering the enable mode. It also verifies if the attempt is successful.

- SSH enable mode password

  Enable mode password is verified while trying to establish connection using SSH and entering the enable mode. It also verifies if the attempt is successful.

After the device credentials are validated the result will be displayed and you can refresh to see the latest status.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Generating Device Credentials Report

You can generate Device Credentials Report from the Report Generator page in RME.

To generate the report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator Page appears.

Step 2 Select Device Credential from the drop-down list on the left.

Step 3 Select either Verification Report or Error report from the drop-down list on the right.

Step 4 Select the required devices using the device selector. (For more details, see the topic, Using RME Device Selector)

Step 5 Select the credentials that you want to verify from the Device Credentials Options pane.

You can select one or many credentials.

Step 6 Click **Finish**.

The generated report appears.

Or

Click **Reset** to clear the selections, and select again.

The following buttons are available on the Credential Verification Report and Credential Error Report:

Button	Description
Export to File (Icon)	Export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.
Export device list to Device Selector (Icon)	Export the list of devices for which the report has been generated, to the Device Selector. You can use this list to perform specific tasks such as, editing the device credentials. You can view this exported list of devices in the Saved device list folder of the RME Device Selector.

You can edit the device credentials by clicking the **Edit Device Credentials** button. This is displayed only if the job has failed devices.

When you click Edit Device Credentials, the Edit Credentials page in DCR is launched. Any changes to the credentials are updated in all the failed devices. A confirmation message is shown before updating credentials in all failed devices.

Credential Verification Report

The Credential Verification Report displays the device names and the credential status for each device. This report can be used to view the static device credential verification report.

The report displays the number of devices that were selected for credential verification, and lists the devices for which the report is not available.

Table 3-11 describes the Credential Verification Report Status messages:

Table 3-11 Understanding Credential Verification Report

Status Message	Description
OK	Check for device credentials completed. The device credentials data in the Device and Credential Repository matches the physical device credentials.
No authentication configured	Device was not configured with authentication mechanism (Telnet/LocalUsername/TACACS). RME was able to telnet and log into the device successfully with out using the values entered in the Device and Credential Repository.
Incorrect	Check for device credentials completed. The device credentials data in the Device and Credential Repository does not match with the physical device credentials for one of the following reasons: • The device credentials data in Device and Credential Repository is not correct. • The device is unreachable or offline. • One of the interfaces on the device is down.
Did Not Try	Check for device credentials is not performed for one of the following reasons: • A Telnet password does not exist, so could not log into the device. • Device Telnet login mode failed, so enable mode login is not attempted.
No Value To Test	Check for device credentials is not performed because you have not entered the device credentials data.
Not Supported	Check for Telnet passwords is not performed because Telnet credential checking is not supported on this device.
Failed	Check failed because a Telnet session could not be established due to a not responding device. Click on the Failed link to view the error message.
Credentials not Verified	Specific credentials were not verified because they were not selected for verification.

The device credentials verification result displays *No Value To Test* for the AUS-managed devices (PIX devices). This is because RME communicates with the AUS using username and password through http protocol.

The SNMP and Telnet or SSH credentials are not required. Any communication to an AUS managed device (PIX devices) does not happen directly, but only through AUS.

Credential Error Report

This is a static device credential verification report. This report lists only those devices where the credentials verification status shows either Failed or Incorrect.

Verifying Device Credentials

To verify device credentials, select **Resource Manager Essentials > Devices > Device Management > Device Credential Verification Jobs**.

The Device Credential Verification Jobs browser dialog box appears with a detailed list of all scheduled CDA jobs.

The columns in the job browser display the following information:

Column	Description
Job ID	Unique number assigned to job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the hyperlink to view the Job details. (See Viewing Job Details)
Status	Status of the job: • Successful—When the job is successful. • Failed—When the job has failed. • Stopped—When the job has been stopped. • Running—When the job is in progress. • Missed Start—When the job is not initiated to run. • Scheduled—When the job is scheduled to run at a later point of time. • Stop Init—When the job is stopped, it goes to Stop Init State before going to Stopped state.
Description	Description of the job, entered at the time of job creation.
Owner	Username of the job creator.
Scheduled at	Date and time at which the job was scheduled.

Column	Description
Completed at	Date and time at which the job was completed.
Schedule Type	Type of job schedule—Immediate, Once, Daily, Weekly, Monthly, 6-Hourly, 12-Hourly. You can specify when you want to run the Device Credential job. To do this, select one of these options from the drop down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. • 6-Hourly—Runs once in 6 hours. • 12-Hourly—Runs once in 12 hours. For periodic jobs, the subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

When you click **Report**, you are taken to the Report Generator Page for Device Credential Verification. (**RME > Reports > Report Generator**).

Click **Create** to to create a new device credential verification job. You must enter the following details:

Device Selector	Select the required devices using Device Selector. (For more details, see Using RME Device Selector)
Device Credentials Options	Select the credential which need to be verified. Click **All** to verify all credentials.
Scheduling	Select the Run Type for the job. If you select Immediate, the job is run immediately. Otherwise, you can select the date and time to run the job.
Job Info	Enter a description for the job. Enter an e-mail id (or multiple e-mail ids) to which the job results have to be sent. You can also specify multiple e-mail ids.

Viewing Job Details

From the Job Browser dialog box, you can learn more about any job by viewing its details.

Step 1 Go to the Device Credential Verification Job Browser and click the Job ID hyperlink.

The Job Details pop-up appears, displaying the day, date and time details in the header at the top of the report. The Job ID and the Status appear in the header of the report.

The Job Details dialog box has two panes. The left pane contains a table of contents for the job results. The results appear in the right pane.

Step 2 Click a page in the left pane to view its corresponding report in the right pane.

Double-click a folder in the left pane to open and close it.

If the folder has subfolders, the next level of subfolders appears under it. Otherwise, its corresponding report appears in the right pane.

The contents of the left pane depends on the state of the job. The left pane can contain:

- Job Summary (in the Job Details folder).
- Devices Details (in the Device Details folder).
- Work Order. Contains same the information as the workorder that was displayed when the job was created.

For retried jobs, the job definitions are not updated. For such jobs, the original job definitions are retained.

To perform actions on a job, click one of the following:

- Edit—Edits selected scheduled job.
- Retry—Retry a failed job. This is applicable for Immediate jobs.
- Stop—Stops or cancels a running job.
- Delete—Deletes the selected job from the job browser.

The following buttons are available in the Job Details page:

Button	Description
Export to File (Icon)	Export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.
Export device list to Device Selector (Icon)	Export the list of devices for which the report has been generated, to the Device Selector. You can use this list to perform specific tasks such as, editing the device credentials. You can view this exported list of devices in the Saved device list folder of the RME Device Selector.

You can edit the device credentials by clicking the **Edit Device Credentials** button. This is displayed only if the job has failed devices.

When you click Edit Device Credentials, the Edit Credentials page in DCR is launched. Any changes to the credentials are updated in all the failed devices. A confirmation message is shown before updating credentials in all failed devices.

After editing the credentials, you can retry the failed jobs.

Device List Manipulation Service

The Device List Manipulation Service (DLMS) allows other network management systems to manipulate Device and Credential Repository devices. You can perform the following, using DLMS:

- Add devices (See Adding Devices to Device Credentials Using DLMS)
- List the RME devices and their status (See Listing the Devices and Their Status Using DLMS)
- Get the device credentials data (See Getting the Device Credentials Data)
- Set the device credentials data (See Setting the Device Credentials Using DLMS)
- Get the device IP address (See Getting the Device IP Address.)

You perform these operations by sending HTTP requests to a special URL. The URL identifies a servlet that accepts the request and authenticates the requesting user's identity and credentials before authorizing the information exchange. The servlet then parses the request, which is encoded in XML, performs the operations, and returns the results in either XML or CSV format (CSV version 3.0).

You must ensure that your HTTP client can create, write, and read sockets.

Create the code to call the following Device List Manipulation Service URL, and pass in the content of the XML file using the HTTP POST method (you can use either Java or PERL):

`http://CiscoWorks-host:port/rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService`

Where,

- *CiscoWorks_host* is the CiscoWorks server hostname.
- The default CiscoWorks port is 1741

To enable secured connection through HTTPS for DLMS, you must configure cmf-app.conf (*NMSROOT*\MDC\Apache\conf) to allow HTTPS access for the servlet rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService:

To configure cmf-app.conf:

Step 1 Add the following text as one line to the file:

```
SetEnvIf Request_URI /rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService
allow_https
```

Step 2 Restart the daemons.

HTTPS access is now enabled.

Create the code to call the following Device List Manipulation Service URL, and pass in the content of the XML file using the HTTPS POST method (you can use either Java or PERL):

`https://``CiscoWorks_host`
`:port/rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService`

Where,

- *CiscoWorks_host* is the CiscoWorks server hostname.
- The default CiscoWorks port is 1741

XML DTD for DLMS

The required XML DTD for the DLMS tool is:

```
<!ELEMENT request
(authentication,source,addDevices?,listDevices?,getDeviceCredentials?,setCredentials?,g
etDeviceIPAddresses?)>

<!ELEMENT authentication EMPTY>

<!ELEMENT source (host,product,version,description)>

<!ELEMENT host (#PCDATA)>

<!ELEMENT product (#PCDATA)>

<!ELEMENT version (#PCDATA)>

<!ELEMENT description (#PCDATA)>

<!ELEMENT addDevices (deviceInfo)>

<!ELEMENT listDevices (deviceInfo?)>

<!ELEMENT getDeviceCredentials (deviceInfo?)>

<!ELEMENT setCredentials (deviceInfo)>

<!ELEMENT getDeviceIPAddresses (deviceInfo?)>

<!ELEMENT deviceInfo (#PCDATA)>

<!ATTLIST request responseFormat  (csv | xml) #IMPLIED>

<!ATTLIST authentication name CDATA #REQUIRED pwd CDATA #REQUIRED>

<!ATTLIST listDevices deviceType (all | managed)  #IMPLIED>

<!ATTLIST getDeviceCredentials wantdbid (yes) #IMPLIED wantsysoid (yes) #IMPLIED>
```

Guidelines for Creating the XML File

The following are the guidelines while creating the DLMS request XML file:

- One request can contain up to five operations.
- You can specify the output as CSV or XML.
- The attribute *pwd* of the tag authentication must be 64-based encoded.
- If you include *deviceInfo* in any operation, you will receive information only on the devices specified in *deviceInfo*. If you do not specify *deviceInfo*, you will receive information on all managed devices. Create *deviceInfo* using CSV format data.

  deviceInfo is the Device Display Name as entered in Device and Credential Repository.
- When using *listDevices*, you can list all devices or only the managed devices by specifying either the *all* or *managed* attribute.
  - You can list all devices by specifying the *attr* as *yes* and *devType* as *all*. If you do not specify this, then only RME managed devices will be displayed.
- When using *getDeviceCredentials*,
  - You can display the device ID by specifying the *wantdbid* attribute as *yes*.
  - You can display the sysobject ID by specifying the *wantsysoid* attribute as *yes*.

Adding Devices to Device Credentials Using DLMS

Using the DLMS function you can add devices to Device and Credentials Repository. After adding devices to Device and Credentials Repository you can add these devices to RME manually or automatically (see Adding Devices to RME).

The new device information should be added using the `deviceInfo` tag.

The CSV version used for adding devices to Device and Credentials is 2.0. You must enter device name (including domain name or simply an IP address) and the SNMP read community string.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The sample XML File for Adding Devices to Device and Credentials Repository (dlmsAddDevices.xml):

```
<source>

<host>CiscoWorks-Server</host>

<product>CiscoWorks:RME</product>

<version>2.0</version>

<description>Using DLMS for adding devices into Device and Credential
Repository</description>

</source>

<addDevices>

<deviceInfo>

<![CDATA[

;

; This file is generated by the export utility

; If you edit this file, be sure you know what you are doing

;

Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv

;

; Here are the columns of the table.

;   Columns 1 and 2 are required.

;   Columns 3 through 20 are optional.

; Col# = 1: Name (including domain or simply an IP)

; Col# = 2: RO community string

; Col# = 3: RW community string

; Col# = 4: Serial Number

; Col# = 5: User Field 1

; Col# = 6: User Field 2

; Col# = 7: User Field 3

; Col# = 8: User Field 4
; Col# = 9; Name = Telnet password

; Col# = 10; Name = Enable password

; Col# = 11; Name = Enable secret

; Col# = 12; Name = Tacacs user

; Col# = 13; Name = Tacacs password

; Col# = 14; Name = Tacacs enable user

; Col# = 15; Name = Tacacs enable password

; Col# = 16; Name = Local user

; Col# = 17; Name = Local password

; Col# = 18; Name = Rcp user

; Col# = 19; Name = Rcp password

; Col# = 20; Name = Group;

; Here are the rows of data.

;

192.168.10.60,public,private,,testdevice,UNKNOWN,0,UNKNOWN,,,,,,,,,,,,

]]>

</deviceInfo>

</addDevices>
```

The example below is a PERL code that calls the DLMS URL and passes in the content of an XML file:

`perl d:\dlms\dlms.pl` *CiscoWorks-Server* **`dlmsAddDevices.xml`**

The DLMS output for adding device is:

```
Authorization succeeded
```

If you have enabled the Automatically Manage Devices from Credential Repository option on the Device Management Settings window then the newly added device is automatically added into RME.

If this option is not enabled, then you have to add device manually to RME from Device and Credential Repository.

See Adding Devices to RME for further details on adding devices into RME from Device and Credentials Repository.

You can also use the DLMS listDevices function to view the newly added device. See Listing the Devices and Their Status Using DLMS for further details.

Listing the Devices and Their Status Using DLMS

Using the DLMS function you can list and view the device status for either:

- All devices in Device and Credential Repository

  Or

- All the RME managed devices.

The device status that are displayed using this tool are managed and unmanaged.

- The devices are considered as managed when they are in RME with one of these device states Normal, Alias, and Pre-deployed.
- The devices are considered as unmanaged when they are in RME with either Conflict or Suspended device states. Also, the devices are considered unmanaged when they are not in RME but in Device and Credentials Repository.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The Sample XML File for Listing the Managed Devices (dlmsListDevices.xml)

```
<?xml version="1.0"?>

<!DOCTYPE request SYSTEM "D:\\dlms\\dtdexternal.dtd">

<request responseFormat="xml">

<!-- the value for responseFormat could be xml or csv -->

<authentication name="admin" pwd='YWRtaW4='/>

<!-- pwd is 64-based encoded -->

<source>

<host>CiscoWorks-Server</host>

<product>CiscoWorks:RME</product>

<version>2.0</version>

<description>Using DLMS for listing devices</description>

</source>

<listDevices attr="yes" deviceType="managed">

</listDevices>
```

The example below is a perl code that calls the DLMS URL and passes in the content of an XML file:

`perl d:\dlms\dlms.pl` *CiscoWorks-Server* **`dlmsListDevices.xml`**

The DLMS output for listing managed devices is:

```
Cisco Systems NM data import, source = List Devices; Version = 2.0; Type = Csv

;

; Here are the columns of the table.

; Col# = 1: Name (including domain or simply an IP)

; Col# = 2: device status

;

; Here are the rows of data.

;

192.168.27.16 -CE 507:managed,

192.168.3.2:managed,

rme-blr-3640.cisco.com:managed,

192.168.3.9-UBR925:managed,
192.168.28.14-CE:managed,
```

To list all the devices in the Device and Credential Repository, change the following line in the given sample XML file:

From

```
<listDevices attr="yes" deviceType="managed">
```

To

```
<listDevices attr="yes" deviceType="all">
```

Getting the Device Credentials Data

Using the DLMS function, you can view the device credentials data for all devices in Device and Credential Repository. The output for getDeviceCredentials is in CSV 3.0 format.

You get the following additional information while using `<getDeviceCredentials>`

- You can get the device ID by specifying the `wantdbid` attribute as *yes*.
- You can get the sysobject ID by specifying the `wantsysoid` attribute as *yes*.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The sample XML File for Geting Device and Credentials for all Devices in Device and Credential Repository (dlmsGetDeviceCredentials.xml):

```
<?xml version="1.0"?>

<!DOCTYPE request SYSTEM "D:\\dlms\\dtdexternal.dtd">

<request responseFormat="xml">

<!-- the value for responseFormat could be xml or csv -->

<authentication name="admin" pwd='YWRtaW4='/>

<!-- pwd is 64-based encoded -->

<source>

<host>CiscoWorks-Server</host>

<product>CiscoWorks:RME</product>

<version>2.0</version>

<description>Using DLMS for getting Device Credentials</description>

</source>

<getDeviceCredentials>

</getDeviceCredentials>
```

The example below is a perl code that calls the DLMS URL and passes in the content of an XML file:

`perl d:\dlms\dlms.pl` *`CiscoWorks-Server`* **`dlmsdlmsGetDeviceCredentials.xml`**

The DLMS output for getting device credentials is:

```
Cisco Systems NM data import, source = Get Devices Credentials; Version = 2.0;
```

```
Type = Csv;
; Here are the columns of the table.
; Col# = 1: Management IP Address
; Col# = 2: Host Name
; Col# = 3: Domain Name
; Col# = 4: Device Identity
; Col# = 5: Display Name
; Col# = 6: SysObjectID
; Col# = 7: DCR Device Type
; Col# = 8: MDF Type
; Col# = 9: SNMP v2 Read Community String
; Col# = 10: SNMP v2 Write Community String
; Col# = 11: SNMP v3 User ID
; Col# = 12: SNMP v3 Password
; Col# = 13: SNMP v3 Engine ID
; Col# = 14: SNMP v3 Auth Algorithm
; Col# = 15: Primary Username
; Col# = 16: Primary Password
; Col# = 17: Primary Enable Password
; Col# = 18: user_defined_field_0
; Col# = 19: user_defined_field_1
; Col# = 20: user_defined_field_2
; Col# = 21: user_defined_field_3
;
; Here are the rows of data.
;
192.168.27.16, , , ,12.19.27.16-CE507,1.3.6.1.4.1.9.1.409,0,268437658,public,private, ,
, , ,admin,default,  , , , ,
192.168.8.9,10.6.8.9, ,
,192.168.8.9-UBR925,1.3.6.1.4.1.9.1.316,0,273900271,public,private, , , , , , ,  , , , ,
```

Setting the Device Credentials Using DLMS

Using the DLMS function you can edit the device credentials for devices specified in <`deviceInfo`> tag.

You can edit the following device credentials:

- snmp_v2_ro_comm_string—SNMP version 2 Read community string
- snmp_v2_rw_comm_string—SNMP version 2 Read-Write community string
- snmp_v3_user_id—SNMP version 3 Username

- snmp_v3_password—SNMP version 3 Password
- snmp_v3_engine_id—SNMP version 3 Engine ID
- snmp_v3_auth_algorithm—SNMP version 3 Authentication Algorithm
- primary_username—Primary Username
- primary_password—Primary Password
- primary_enable_password—Primary Enable Password
- user_defined_field_0—User-defined field
- user_defined_field_1—User-defined field
- user_defined_field_2—User-defined field
- user_defined_field_3—User-defined field

The following table describes the mapping of CSV 2.0 to CSV 3.0

CSV 2.0	**CSV 3.0**
Name (including domain or simply an IP)	host_name and display_name
RO community string	snmp_v2_ro_comm_string
RW community string	snmp_v2_rw_comm_string
Serial Number	Not used in CSV 3.0
User Field 1	user_defined_field_0
User Field 2	user_defined_field_1
User Field 3	user_defined_field_2
User Field 4	user_defined_field_3
Telnet password	primary_password
Enable password	primary_enable_password
Enable secret	primary_enable_password
Tacacs user	primary_username

CSV 2.0	CSV 3.0
Tacacs password	primary_password
Tacacs enable user	Not used in CSV 3.0
Tacacs enable password	primary_enable_password
Local user	primary_username
Local password	primary_password
Rcp user	Not used in CSV 3.0
Rcp password	Not used in CSV 3.0

The order of preference used to set these values in CSV 3.0 are:

- If Tacacs username, password, enable password is set, these values will be set as primary_username, primary_password and primary_enable_password.
- If Local username and password is set, then the values will be set as primary_username and primary_password.
- If Telnet password, Enable Password, and Enable Secret are set, then the values will be set as primary_password, and primary_enable_password (for both Enable Password, and Enable Secret).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The sample XML File for Editing Device and Credentials for all Devices in Device and Credential Repository (dlmsSetDeviceCredentials.xml):

```
<?xml version="1.0"?>

<!DOCTYPE request SYSTEM "D:\dlms\dtdexternal.dtd">

<request responseFormat="xml">

<!-- the value for responseFormat could be xml or csv -->

<authentication name="admin" pwd='YWRtaW4='/>

<!-- pwd is 64-based encoded -->

<source>

<host>ramyab-w2k07</host>

<product>CiscoWorks:RME</product>

<version>2.0</version>

<description>using DLMS for device manipulation in RME</description>

</source>

<setCredentials>

<deviceInfo>

<![CDATA[

;

; This file is generated by the export utility

; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv
;
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 13 are optional.
; Col# = 1:  Name (including domain or simply an IP)
; Col# = 2:  snmp_v2_ro_comm_string
; Col# = 3:  snmp_v2_rw_comm_string
; Col# = 4:  snmp_v3_user_id
; Col# = 5:  snmp_v3_password
; Col# = 6:  snmp_v3_auth_algorith
; Col# = 7:  primary_username
; Col# = 8:  primary_password
; Col# = 9:  primary_enable_password
; Col# = 10: user_defined_field_0
; Col# = 11: user_defined_field_1
; Col# = 12: user_defined_field_2
; Col# = 13: user_defined_field_3
;
; Here are the rows of data.
;
rtr1750,dlmstest,invtest,snmpv3user,snmpv3pass,11111111111111,MD5,puser,ppass,enable,uf
1,uf2,uf3,uf4
]]>
</deviceInfo>
</setCredentials>
```

The example below is a perl code that calls the DLMS URL and passes in the content of an XML file:

`perl d:\dlms\dlms.pl` *`CiscoWorks-Server`* **`dlmsdlmsSetDeviceCredentials.xml`**

The DLMS output for editing the device credentials is:

```
Authorization succeeded
```

You can verify the result by any of the following methods:

- Select **Common Services > Device and Credentials > Device Management > Export** (button)
- Select **Resource Manager Essentials > Devices > Device Management > RME Devices > Export** (button)
- Using the DLMS **`getDeviceCredentials`** function. See Getting the Device Credentials Data for further details.

Getting the Device IP Address

Using the DLMS function you can get the device IP address of the specified devices.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The sample XML File for Editing Device and Credentials for all Devices in Device and Credential Repository (dlmsGetDeviceIPaddress.xml):

```
<?xml version="1.0"?>

<!DOCTYPE request SYSTEM "D:\\dlms\\dtdexternal.dtd">

<request responseFormat="xml">

<!-- the value for responseFormat could be xml or csv -->

<authentication name="admin" pwd='YWRtaW4='/>

<!-- pwd is 64-based encoded -->

<source>

<host>CiscoWorks-Server</host>

<product>CiscoWorks:RME</product>

<version>2.0</version>

<description>Using DLMS for getting the device IP Address</description>

</source>

<getDeviceIPAddresses>

<!-- <![CDATA[ ... ]]> is needed for the text holding special charactors, such as &, <, >,

', ", -->

</getDeviceIPAddresses>
```

The example below is a perl code that calls the DLMS URL and passes in the content of an XML file:

```
perl d:\dlms\dlms.pl CiscoWorks-Server dlmsdlmsSetDeviceCredentials.xml
```

The DLMS output for getting the device IP address is:

```
Cisco Systems NM data import, source = Get Devices IP Addr; Version = 2.0; Type

= Csv

;

; Here are the columns of the table.

; Col# = 1: Name (including domain or simply an IP)

; Col# = 2 or above: IP addresses

;

; Here are the rows of data.

;

CE-507:192.168.27.16,

192.168.38.9-UBR925:192.168.38.9,
rme-3640.cisco.com:192.168.28.19
```

Sample DLMS XML Request File

This is an example of XML code requesting all five Device List Manipulation Service operations (show.xml).

This example also includes the XML DTD used for DLMS.

```
<?xml version = '1.0' ?>

<!DOCTYPE request [

<!ELEMENT request
(authentication,source,addDevices?,listDevices?,getDeviceCredentials?,setCredentials?,r
enameDevices?,deleteDevices?,getDeviceIPAddresses?)>

<!ELEMENT authentication EMPTY>

<!ELEMENT source (host,product,version,description)>

<!ELEMENT host (#PCDATA)>

<!ELEMENT product (#PCDATA)>

<!ELEMENT version (#PCDATA)>

<!ELEMENT description (#PCDATA)>

<!ELEMENT addDevices (deviceInfo)>

<!ELEMENT listDevices (deviceInfo?)>

<!ELEMENT getDeviceCredentials (deviceInfo?)>

<!ELEMENT setCredentials (deviceInfo)>

<!ELEMENT renameDevices (deviceInfo)>

<!ELEMENT deleteDevices (deviceInfo)>

<!ELEMENT getDeviceIPAddresses (deviceInfo?)>

<!ELEMENT deviceInfo (#PCDATA)>

<!ATTLIST request

responseFormat CDATA #IMPLIED>

<!ATTLIST authentication

name CDATA #REQUIRED

pwd CDATA #REQUIRED>

<!ATTLIST listDevices

deviceType CDATA #IMPLIED>

<!ATTLIST getDeviceCredentials

wantdbid CDATA #IMPLIED

wantsysoid CDATA #IMPLIED>

<!ATTLIST deleteDevices suspend CDATA #IMPLIED>

]>

<request responseFormat="xml">
```

```
<!-- the value for responseFormat could be xml or csv -->
<authentication name="admin" pwd='YWRtaW4='/>
<!-- pwd is 64-based encoded -->
<source>
<host>CiscoWorks-Server</host>
<product>CiscoWorks:RME</product>
<version>2.0</version>
<description>text by caller</description>
</source>
<addDevices>
<!-- <![CDATA[ ... ]]> is needed for the text holding special charactors, such as &, <,
>, ', ", -->
<deviceInfo><![CDATA[
; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv
;
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 19 are optional.
; Col# = 1: Name (including domain or simply an IP)
; Col# = 2: RO community string
; Col# = 3: RW community string
; Col# = 4: Serial Number
; Col# = 5: User Field 1
; Col# = 6: User Field 2
; Col# = 7: User Field 3
; Col# = 8: User Field 4
; Col# = 9; Name = Telnet password
; Col# = 10; Name = Enable password
; Col# = 11; Name = Enable secret
; Col# = 12; Name = Tacacs user
; Col# = 13; Name = Tacacs password
; Col# = 14; Name = Tacacs enable user
; Col# = 15; Name = Tacacs enable password
; Col# = 16; Name = Local user
; Col# = 17; Name = Local password
; Col# = 18; Name = Rcp user

; Col# = 19; Name = Rcp password

;

; Here are the rows of data.

;

enm-2501.cisco.com,public,private

enm-4888.cisco.com,public,priv,Big Boys1,field2,,,,,,,,,,,,,rcp2,rcppwd2

enm-8333.cisco.com,public,private

enm-4001.cisco.com,public,private,Big Boys1,,,,,,,,,,,,,,rcp2,rcppwd2

enm-7010.cisco.com,public,private,Big Boys1,,,,,,,,tacuser3,tacpwd3

192.168.5.6,"public,I am
,",public,sn2512,my_anno1,my_anno2,my_anno3,my_anno4,,,,tacuser1,tacpwd1,tacuser2,tacpw
d2,,,rcp1,rcppwd1

]]></deviceInfo>

</addDevices>

<listDevices>

<deviceInfo><![CDATA[

; This file is generated by the export utility

; If you edit this file, be sure you know what you are doing

;

Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv

;

; Here are the columns of the table.

; Columns 1 and 2 are required.

; Columns 3 through 19 are optional.

; Col# = 1: Name (including domain or simply an IP)

; Col# = 2: RO community string

; Col# = 3: RW community string

; Col# = 4: Serial Number

; Col# = 5: User Field 1

; Col# = 6: User Field 2

; Col# = 7: User Field 3

; Col# = 8: User Field 4

; Col# = 9; Name = Telnet password

; Col# = 10; Name = Enable password

; Col# = 11; Name = Enable secret

; Col# = 12; Name = Tacacs user

; Col# = 13; Name = Tacacs password
; Col# = 14; Name = Tacacs enable user
; Col# = 15; Name = Tacacs enable password
; Col# = 16; Name = Local user
; Col# = 17; Name = Local password
; Col# = 18; Name = Rcp user
; Col# = 19; Name = Rcp password
;
; Here are the rows of data.
;
;enm-4000.cisco.com
;enm-7010.cisco.com
;192.168.5.9
mytest.cisco.com
good
;bad
]]></deviceInfo>
</listDevices>
<getDeviceCredentials wantsysoid="yes" wantdbid="yes">
<deviceInfo>
; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv
;
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 19 are optional.
;; Col# = 1: Management IP Address \n"
; Col# = 2: Host Name \n"
; Col# = 3: Domain Name \n"
; Col# = 4: Device Identity \n"
; Col# = 5: Display Name \n"
; Col# = 6: SysObjectID \n"
; Col# = 7: DCR Device Type \n"
; Col# = 8: MDF Type \n"
; Col# = 9: SNMP v2 Read Community String \n"
; Col# = 10: SNMP v2 Write Community String \n"
; Col# = 11: SNMP v3 User ID \n"
; Col# = 12: SNMP v3 Password \n"
; Col# = 13: SNMP v3 Engine ID \n"
; Col# = 14: SNMP v3 Auth Algorithm \n"
; Col# = 15: Primary Username \n"
; Col# = 16: Primary Password \n"
; Col# = 17: Primary Enable Password \n"
; Col# = 18: user_defined_field_0 \n"
; Col# = 19: user_defined_field_1 \n"
; Col# = 20: user_defined_field_2 \n"
; Col# = 21: user_defined_field_3 \n"
;
; Here are the rows of data.
;
enm-2501.cisco.com
enm-2502.cisco.com
enm-2503
enm-7010.cisco.com
12.18.5.9
</deviceInfo>
</getDeviceCredentials>
<setCredentials>
<!-- <![CDATA[ ... ]]> is needed for the text holding special charactors, such as -->
<deviceInfo><![CDATA[
; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
;
Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv
;
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 19 are optional.
; Col# = 1: Name (including domain or simply an IP)
; Col# = 2: snmp_v2_ro_comm_string
; Col# = 3: snmp_v2_rw_comm_string
; Col# = 4: snmp_v3_user_id
; Col# = 5: snmp_v3_password
; Col# = 6: snmp_v3_auth_algorith
; Col# = 7: primary_username
; Col# = 8: primary_password
; Col# = 9: primary_enable_password
; Col# = 10: user_defined_field_0
; Col# = 11: user_defined_field_1
; Col# = 12: user_defined_field_2
; Col# = 13: user_defined_field_3
;
; Here are the rows of data.
;
enm-2501.cisco.com,public,private,serial,field1,fidel2,fild3
enm-4888.cisco.com,public,priv,little Boys1,field2,,,,,,,,,,,,,rcp9,rcppwd9
enm-4001.cisco.com,public,private,Big Boys1,,,,,,,,,,,,,rcp2,rcppwd2
enm-7010.cisco.com,public,private,Big Boys1,,,,,,,,tacuser3,tacpwd3
;192.168.5.9,"public,I am
,",public,sn2512,my_anno1,my_anno2,my_anno3,my_anno4,,,,tacuser1,tacpwd1,tacuser2,tacpw
d2,,,rcp1,rcppwd1
mytest.cisco.com,public,private
]]></deviceInfo>
</setCredentials>
<getDeviceIPAddresses>
<deviceInfo>
</deviceInfo>
</getDeviceIPAddresses>
</request>
```

Sample Java and PERL Scripts to Invoke the Servlet

The section captures Java and PERL code examples that call the DLMS URL and passes in the content of an XML file.

- Java Example
- PERL Example

Java Example

This is an example of Java code that calls the Device List Manipulation Service URL and passes in the content of an XML file.

```
import java.util.*;
import java.io.*;
import java.net.*;
import javax.servlet.*;
import javax.servlet.http.*;
```

```
public class UseDevListSvc extends HttpServlet {

public synchronized void doGet(HttpServletRequest req, HttpServletResponse res)

throws ServletException, IOException {


res.setContentType("text/plain");

PrintWriter pw = res.getWriter();

int port = req.getServerPort();

String host = req.getServerName();;

// Make sure you put show.xml in the right directory. the default

// is CSCOpx/example .

String filename = "/opt/CSCOpx/example/show.xml";

String paramList = fileToString(filename, pw);

String URL = "/rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService";

try {

DataInputStream ds = execPOST(host, port, URL, paramList, pw);

if (ds == null) {

throw new Exception("Could not contact URL " + URL+ " with "+paramList); }

BufferedReader br = new BufferedReader(new InputStreamReader(ds));

String line = null;

while ((line = br.readLine()) != null ){

if (line.indexOf("-1:") > 0 ) { //this indicates an error.

throw new Exception("Received result " + line );

}

pw.println(line);

}

} catch (Exception e) {

pw.println("Error in doGet: "+ e.getMessage());

}

pw.flush();

pw.close();

}

public static DataInputStream execPOST(String Host,int Port, String URI, String data,
PrintWriter pw) {

URL url = null;

URLConnection urlConn;

DataOutputStream printout;

try {

if (Port == -1) {
```

```
url = new URL ("http://" + Host +URI);
} else {
url = new URL ("http", Host, Port, URI);
}
urlConn = url.openConnection();
urlConn.setDoInput (true);
urlConn.setDoOutput (true);
urlConn.setUseCaches (false);
urlConn.setDefaultUseCaches (false);
urlConn.setRequestProperty
("Content-Type", "application/x-www-form-urlencoded");
printout = new DataOutputStream (urlConn.getOutputStream ());
if (data != null)
printout.writeBytes(data);
printout.flush();
printout.close();
return new DataInputStream (new BufferedInputStream( urlConn.getInputStream ()));
}catch (Exception e) {
pw.println("Error in execPOST: "+ e.getMessage());
return null;
}
}
private String fileToString (String filename,  PrintWriter pw) {
InputStream is = null;
String out = "";
try {
is = new FileInputStream(filename);
} catch (FileNotFoundException notFound) {
pw.println("Error in fileToString: " + notFound.getMessage());
return null;
}
if (is == null) pw.println("read nothing from the file");
else pw.println("read ok from the xml file.");
try {
InputStreamReader isr = new InputStreamReader(is);
BufferedReader br = new BufferedReader(isr);
String line;
while((line = br.readLine()) != null) {
```

```
out = out + line + "\n";

}

} catch (IOException e) {

pw.println("Error in fileToString: " + e.getMessage());

return null;}

return out;}

public synchronized void doPost(HttpServletRequest req, HttpServletResponse res)

throws ServletException, IOException {

doGet(req,res);}

}
```

PERL Example

This is an example of PERL code that calls the Device List Manipulation Service URL and passes in the content of an XML file.

```
#!/opt/CSCOpx/bin/perl

# Sample perl script to use Device List Manipulation API.
# The return information from the API is printed out to STDOUT.

use LWP::UserAgent;

my $myInput = "";
my $url;

my $DevListSvc = '/rme/com.cisco.nm.rmeng.inventory.servlet.DeviceListService';
my $fileLoc = "/opt/CSCOpx/example/show.xml";
my $server = 'CiscoWorks-Server';

my $port = '1741';

open xmlFILE, $fileLoc or die "Can't find file $fileLoc: $!\n";
while (<xmlFILE>) {
$myInput .= $_;
}

$url = 'http://' . $server . ':' . $port . $DevListSvc;

$ua = new LWP::UserAgent;
$ua->agent("AgentName/0.1 " . $ua->agent);

### Create a request
my $request = new HTTP::Request POST => $url;
$request->content_type('application/x-www-form-urlencoded');
$request->content($myInput);

my $response = $ua->request($request);

### Check the outcome of the response
if ($response->is_success) {
```

```
print $response->content;
### or do other data processing with the response outcome.

} else {

print "The request is failed\n";

}
```

Device Manageability Status

You can verify device manageability status using Device Manageability Status option. This option enables you to generate a Device Manageability Status report to identify possible causes for Inventory and Configuration collection failure and take timely corrective action.

To generate a Device Manageability Status Report:

Step 1 Select **Resource Manager Essentials > Devices > Device Management > Device Manageability Status**

The RME Device Manageability Status dialog box appears.

Step 2 Select the required devices using the Device Selector. (See the topic, Using RME Device Selector for more details.)

Step 3 Click on **Generate Report** button to generate a Device Manageability Status Report.

Understanding Device Manageability Status Report

Table 3-12 lists and describes the various fields that constitute a Device Manageability Status Report.

Table 3-12 Fields in a Device Manageability Status Report

Field	Description
Device Name	Device Display Name of the device as entered in Device and Credential Repository.
Sys Object Id	sysObjectID of the device. sysObjectID is an authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining the kind of box that is managed.
Model	Model of the device
Device Status	Device status is either Managed or Unmanaged. • The devices are Managed when they are in RME in any of these device states: Normal, Alias, and Pre-deployed. • The devices are Unmanaged when they are in RME in either of these device states: Conflict or Suspended device states. The devices are also considered Unmanaged when they are not in RME but in Device and Credentials Repository.

Table 3-12 Fields in a Device Manageability Status Report

Field	Description
Inventory Collection Status	Inventory Collection status of a device can be either Success or Failed. • The collection is considered successful, if all the required information about the device is received by the RME server. • The collection is considered as Failed, if all the required information about the device is not received by the RME server. If the status of Inventory Collection is Failed, then the possible causes as well as the recommended corrective actions are provided for the device.
Inventory Last Updated time	Time at which the Inventory Collection was last run.
Config Collection Status	The Configuration collection status of a device can be either Success or Failed. • The collection is considered Successful, if all the required information about the device is received by the RME server. • The collection is considered as Failed, if all the required information about the device is not received by the RME server. Click on Success or Failed link against each device to get detailed information of the reasons for Config collection success or failure..
Config Last Updated time	The time at which the Configuration collection was last run.

Note During Upgrade or Restore, the generated Device Manageability Status report may not display data for some devices. You need to run a fresh Inventory or Configuration collection for those devices and generate the report again.

Using RME Device Selector

The Device Selector pane is used to select RME devices to perform RME tasks. This pane lists all RME devices in a group. The devices are listed in the appropriate groups based on Device type groups and User-defined group rules.

The devices name that you see in this pane is the Display Name that you have entered at the time of adding the devices in Device and Credential Repository.

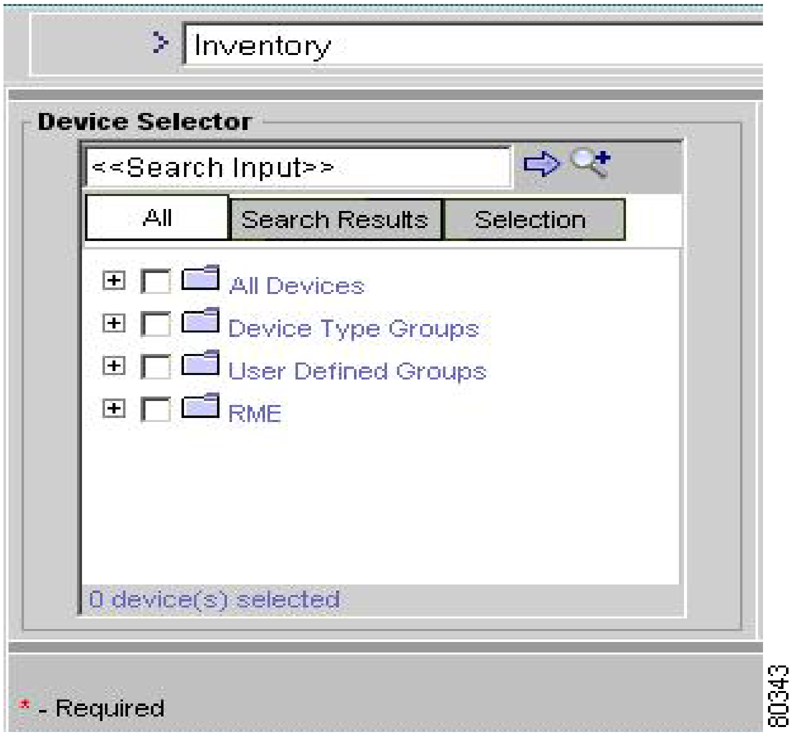
Note If you have configured CiscoWorks login mode to work under ACS mode (**Common Services > Server > Security > AAA Mode Setup**), the devices listed for you while performing the RME tasks are based on your role and associated privileges that are defined in Cisco Secure ACS.

The Device Selector pane contains the following fields or buttons:

Field/Button	Description
Search Input	Enter the search expression in this field. You can enter single device names or multiple device names. If you are entering multiple device names, separate them with a comma. You can also enter the wildcard characters “*” amd "?". For example: 192.168.10.1*, 192.168.20.*
Search	Use this icon to perform a simple search of devices based on the search criteria you have specified in the Search Input text field. For information on Search, see Using Simple Search.
Advanced Search	Use this icon to perform an advanced search of devices based on the search criteria you have specified in the Search Input text field. For information on Advanced Search, see Using Advanced Search.
All	Lists all User-defined and System-defined groups for all applications that are installed on CiscoWorks server. For more information, see Using the All Tab.
Search Results	Displays all the search results from Search or Advanced Search. For more information, see Using the Search Results Tab.
Selection	Lists all the devices that you have selected in the Search Results or All tab. Using this tab, you can deselect devices from the list. For more information, see Using the Selection Tab.

Figure 3-1 shows the new device selector.

Figure 3-1 Device Selector


Inventory
Device Selector
<<Search Input>>
All
Search Results
Selection
All Devices
Device Type Groups
User Defined Groups
RME
0 device(s) selected
* - Required
80343

Tool-tips are provided for long device names so that you do not have to scroll to see the complete device name.

Using Simple Search

You can search for devices by entering the devices name (Display Name) in the Search Input field.

The search is based on the Display Name that you view in the Device Selector pane. This Display Name is entered when you add devices to Device and Credential Repository (**Common Services > Device and Credentials > Device Management**).

Usage Notes

The following are the usage notes for Simple Search:

- You can enter multiple device names separated with a comma. You can also enter wildcard character, "*" or "?" for selecting multiple devices.

  For example:

  You can enter device names in these many ways to select multiple devices:

  - 192.168.80.140, 192.168.135.101, rtr805
  - 192.168.80.*, 192.168.*
  - 192.168.22.?

  You cannot enter multiple wildcard characters for selecting the devices

  For example, 192.*.80.*. This is not allowed.

- You must enter either the complete device name or enter the partial device name appended with wildcard character *. That is,
  - No devices are selected, if you enter only 192.168 in the Device Name text box.
  - You have to enter either 192.168* or 192.168.10.10.
- The search is not case-sensitive.
- The devices that are selected is a unique list. There are no duplicate entries of devices.

  For example:

  If you have these devices in All Devices and Normal devices nodes: 192.168.10.10, 192.168.10.20, 192.168.10.21, 192.168.10.30, and 192.168.10.31 then,

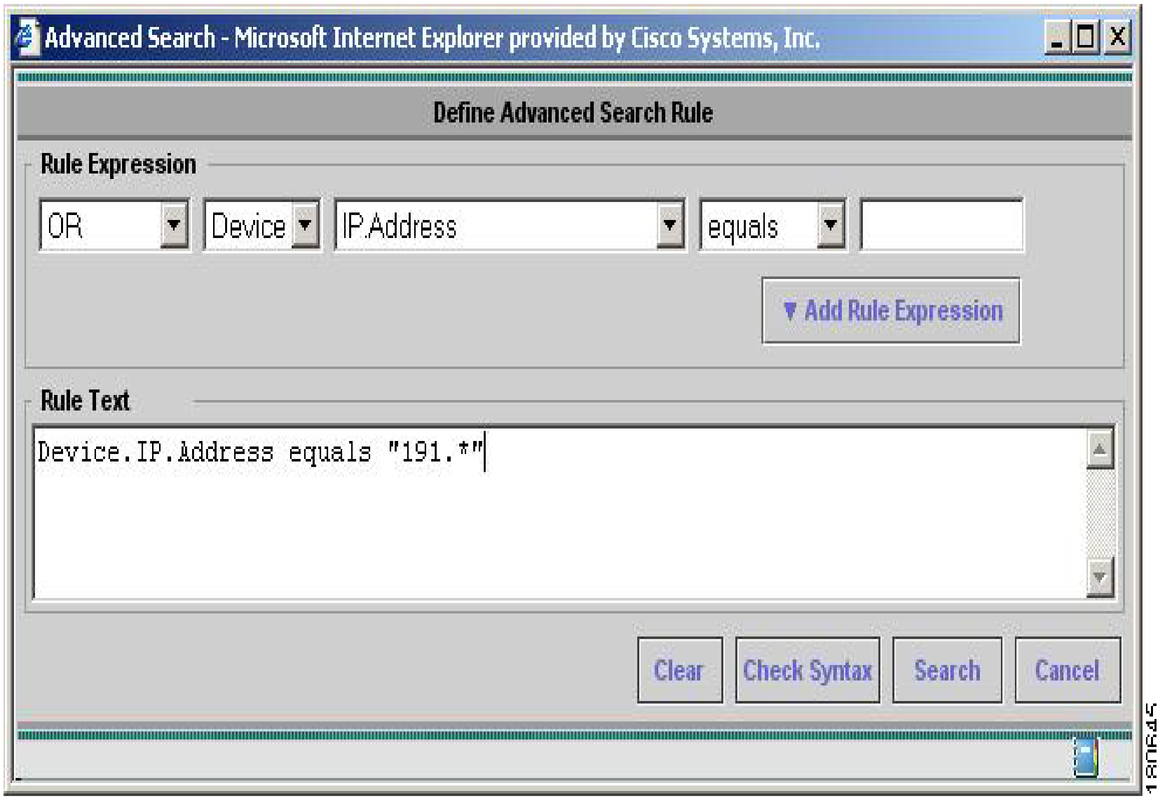
  a. Select the devices 192.168.10.20, 192.168.10.21, and 192.168.10.30 in the Normal devices node.
  b. Enter the search criteria 192.168.10.2*
  c. The final selected devices that is displayed is, 192.168.10.20, 192.168.10.21, and 192.168.10.30 in the Normal devices node and 192.168.10.20 and 192.168.10.21 in All Devices node. However, the selected devices count that is displayed in the Device Selector is only three and not five.
- The All Devices node is expanded without selecting any devices, if the search criteria is not satisfied. The object(s) selected text displays 0 (zero) device selected.

Using Advanced Search

You can use the Advanced Search icon to specify a set of rules for advanced search. Advanced search is based on the Grouping Services attributes of RME's Grouping Services Server. In the Advanced Search dialog box, you can create rules to search for devices.

Figure 3-2 shows the Advanced Search dialog box.

Figure 3-2 Device Selector Advanced Search


Advanced Search - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Define Advanced Search Rule
Rule Expression
OR
Device
IP.Address
equals
▼ Add Rule Expression
Rule Text
Clear
Check Syntax
Search
Cancel
180645

Device.IP.Address equals "191.*"

This dialog box contains the following fields and buttons :

Field/Buttons	Description
OR, AND, EXCLUDE	Logical operators. • OR—Include objects that fulfill the requirements of either rule. • AND—Include only objects that fulfill the requirements of both rules. • EXCLUDE—Do not include these objects. This field appears only after a rule expression is added in the Rule Text box.
Object Type	The type of object (device) that is used to form a group. All RME rule expressions begin with the same Object Type, RME:INVENTORY:Device.
Variable	Device attributes, based on which you can define the group. See RME Advanced Search Rule Attribute.
Operator	The operator to be used in the rule. The list of possible operators changes based on the Variable selected.

Field/Buttons	Description
Value	The value of the rule expression. The possible values depend upon the variable and operator selected. Depending on the operator selected, the value may be free-form text or a list of values. The wildcard characters are not supported.
Add Rule Expression	Used to add the rule expression to the group rules.
Rule Text	Displays the rule.
Check Syntax	Verifies that the rule syntax is correct. Use this button if you have entered the rules manually.
Search	Used to search for devices based on the defined rule.

Usage Notes

The following are the usage notes for Advanced Search:

- If you have not selected any device nodes, then advanced search is applied only for All Devices node.
- You can either enter the rules directly in the Rule Text field, or select the components of the rule from the Rule Expression fields, and form a rule.

  Each rule expression contains the following:

  object type.variable operator value

  Object Type—The type of object (device) that is used to form a group. All RME rule expressions begin with the same Object Type, RME:INVENTORY:Device.

  Variable—Device attributes, based on which you can define the group. See the RME Advanced Search Rule Attribute.

  Operator—Operator to be used in the rule. The list of possible operators changes based on the Variable selected.

  Value—Value of the rule expression. The possible values depend upon the variable and operator selected. Depending on the operator selected, the value may be free-form text or a list of values.
- If you are entering the rule expressions manually, the rule expression must follow this syntax:

  object type.variable operator value
- If you are entering more than one rule expression, you must enter logical operators OR, AND or EXCLUDE after every rule expression.

  You must use Check Syntax button only when you add a rule manually or when you modify a rule expressions in the Rule Text.
- The advanced search operation is not case-sensitive.
- To delete the rules in the Rule Text box, select the complete rule including the logical operator and press the Delete key on your keyboard.
- If you want to perform a new search, click **Clear All** before selecting any new devices.

RME Advanced Search Rule Attribute

Table 3-13 lists the available device advanced search rule attributes that you can use for defining advanced search.

Table 3-13 RME Advanced Search Rule Attribute

Attribute Group	Attribute Type	Description
Asset	Asset.CLE_Identifier	CLE identifier of the asset.
	Asset.Part_Number	Orderable part number of the asset.
	Asset.User_Defined_Identifier	User-defined identifier of the asset
Chassis	Chassis.Model_Name	Name of the model.
	Chassis.Number_Of_Slots	Number of slots in that chassis.
	Chassis.Port_Count	Total port count of the chassis.
	Chassis.Serial_Number	Serial number of the chassis.
	Chassis.Vendor_Type	Type of vendor for the chassis.
	Chassis.Version	Version number of the chassis.
Flash	Flash.File_Name	Name of the flash file.
	Flash.File_Size	Flash file size in MB.
	Flash.Model_Name	Model name of the flash device.
	Flash.Partition_Free	Free space in MB.
	Flash.Partition_Name	Flash partition name.
	Flash.Partition_Size	Flash partition size in MB.
	Flash.Size	Total flash device size in MB.
Image	Image.ROM_Sys_Version	ROM system software version
	Image.ROM_Version	Version of ROM.
	Image.Sys_Description	Image system description
	Image.Version	Running image version.
IP Address	IP.Address	Device IP address.
	IP.Address_Type	Version of IP, IPv4 or IPv6
	IP.Network_Mask	Network Mask address
Memory	Memory.Free	Free memory in MB.
	Memory.Name	Name of the memory.
	Memory.Size	Total RAM size in MB.
	Memory.Type	Memory type.
	Memory.Used	Used memory in MB.
Module	Module.HW_Version	Module hardware version.
	Module.Model_Name	Name of the model.
	Module.Port_Count	Total ports on that module.
	Module.Serial_Number	Serial number of the module.
	Module.Vendor_Type	Type of vendor for the module.

Table 3-13 RME Advanced Search Rule Attribute (continued)

Attribute Group	Attribute Type	Description
Processor	Processor.Model_Name	Name of the model.
	Processor.NVRAM_Size	Size of the processor NVRAM in MB.
	Processor.NVRAM_Used	Size of the processor NVRAM that has been utilized, in MB.
	Processor.Port_Count	Total port count of the processor
	Processor.RAM_Size	Size of the processor RAM in MB.
	Processor.Serial_Number	Serial number of the processor.
	Processor.Vendor_Type	Type of vendor for the processor.
State	State	RME device state such as Normal, Alias, etc.
System	System.Contact	Device contact person name.
	System.Description	Description of the system.
	System.DomainName	Device domain name.
	System.Location	Device location information.
	System.SystemOID	System Object ID of the device (sysObjectID).

Using Advanced Search—An Example

The following example describes the procedure for selecting devices whose IP address starts with 192.168 or Network Mask is 255.255.255.0. Also, these devices are assumed to be in Normal state.

The devices in your network are:

- 192.168.101.200 with network mask 255.255.255.128
- 192.168.101.201 with network mask 255.255.255.0
- 192.168.102.251 with network mask 255.255.255.0
- 192.168.102.202 with network mask 255.255.255.19
- 192.168.200.210 with network mask 255.255.255.128

Use the following procedure for Advanced search:

Step 1 Click the Advanced Search icon in the Device Selector pane.

The Define Advanced Search Rule dialog box appears.

Step 2 Select,

a. State as Variable

b. = as Operator

c. Normal as Value

Step 3 Click **Add Rule Expression**.

The rule is added into the Rule Text.

Step 4 Select,

a. And as Logical Operator

b. IP.Address as Variable

c. Contains as Operator

d. Enter 192.168.101 for Value.

Step 5 Click **Add Rule Expression**.

The rule is added into the Rule Text.

Step 6 Select,

a. OR as Logical Operator

b. IP.Network_Mask as Variable

c. equals as Operator

d. Enter 255.255.255.0 for Value.

Step 7 Click **Add Rule Expression**.

The rule is added into the Rule Text.

Step 8 Click **Search**.

The Device Selection dialog box appears.

The devices that satisfied the search condition are selected. That is these two devices are selected.

- 192.168.101.200 with network mask 255.255.255.128
- 192.168.101.201 with network mask 255.255.255.0
- 192.168.102.251 with network mask 255.255.255.0

Using the All Tab

The All tab lists all the devices that are available in the RME. The list is based on the Display Name that you entered in the Device Properties dialog box when you added devices to Device and Credential Repository (**Common Services > Device and Credentials > Device Management**).

List of Device Folders

The following is the list of device folders under the All tab:

- The All Devices folder lists all RME devices. That is, this includes devices in Normal, Alias, Pending, and Pre-deployed states. This folder does not include devices in Suspended and Conflicting states.
- The Normal Devices folder lists RME devices that has been successfully contacted by RME or the device has contacted RME at least once (polling, successful job completion, Syslog receipt etc.).
- The Pre-deployed folder lists RME Device has never ever been reachable by RME (by protocol such as SNMP).
- The Previous selection folder lists RME devices that were selected in previous RME task in the same session.
- Saved device list folder lists RME devices that are saved explicitly by you while generating the Inventory Reports (**Reports > Generator**), View Credential Verification Report and Error Report **(Devices > Device Management > Device Credential Verification)**.

Only one Saved device list is created within the RME device selector. If concurrent users have created Saved device list, only the last created Saved device list appears in the RME Device Selector. The previous Saved device list is overwritten with the latest.

You can use the Previous selection and Saved device groups only when you are working on a RME application. You cannot use these device groups when you are working on another CiscoWorks application. That is, if you are working on the Campus Manager application, these groups must not be used.

- The User Defined Groups folder lists RME devices that satisfy the group rules. The group rules are defined by you at the time of creating the User-defined groups.

  See Managing RME Device Groups Using Group Administration for further details on RME User-defined groups.

- Based on the applications that are installed on your CiscoWorks server, you will also view device folders related to other CiscoWorks applications:
  CiscoWorks_ApplicationName@CiscoWorks_ServerHostName

  For example: For CiscoWorks Common Services, you will see:

  CS@*CiscoWorks_ServerHostName.*

  In a stand-alone system, server name is not appended. For example, for Common Services, you will see CS.

- Other application folders are displayed in RME based on the settings at Common Services > Device Management > Device Selector Settings. For more details, see Common Services Online Help.

- In RME Device Selector, the other CiscoWorks application device folders will list only RME devices.

  For example: If you have devices, A, B, C and D in CiscoWorks Common Services and you have devices A, B, and C in RME then in the RME Device Selector under Common Services device folder, you will view on RME device list, A, B, and C.

- The device appears in a disabled (greyed out) state when:
  - Device type is *Unknown* in Device and Credential Repository. In all RME applications device is shown as disabled except in Inventory job creation and reports.
  - Device type is known and correct in Device and Credentials (that is, the SysObjectID is correct and is available in Device and Credentials). However, that device is not supported by RME applications. (Inventory, Software Management, and Configuration Management).

There are two types of device selectors in RME:

- Single Device Selector
- Multiple Device Selector

Single Device Selector

In the single device selector, you can select a device only at the leaf-level (device-level). The radio buttons at the node-level (folder-level) are grayed out.

Multiple Device Selector

In the multiple device selector, you can select devices at both the node-level and leaf-level.

The following are the usage notes for the multiple device selector:

- If you select devices at the node-level, all devices listed under this node are selected.

  For example, if you select the All Devices node, all devices under this node are selected.

- If you expand a device node, you cannot select devices at the node-level. You need to select devices individually at the leaf-level.

  For example, if you expand the All Devices node, you cannot select devices at the All Devices node-level (the check-box is grayed out). You need to select devices individually under the All Devices node.
- If you select devices at a node-level and expand that particular node, you can deselect the devices only at the leaf-level and not at the node-level.

  For example, if you select the Normal Devices node and expand the same, you can deselect the devices only at the leaf-level. You cannot deselect all the devices at the Normal Devices node-level (the check-box is grayed out), when it is expanded. However, you can use **Clear All** to deselect all the devices.
- You can select multiple device nodes to perform the RME tasks.

  For example, you can select the Previous selection and the Saved device list nodes together to perform the RME tasks.

Using the Search Results Tab

The Search Results Tab lists all the results of Simple search or advanced search operations. It displays a flat list of devices and you can do a select all , clear all , or select a few devices from the list.

Using the Selection Tab

The Selection Tab serves as a repository of all the devices that you select from the Search Results tab or the All Tab.

There are three ways to select devices in the Device Selector:

- Selection Using All Tab
- Selection Using Search
- Selection Combining All and Search

Selection Using All Tab

You can select devices using the tree view in the All tab. This tab displays all devices that are available in RME.

Selection Using Search

You can search devices using Search or Advanced Search. The list of devices matching the search criteria is shown under the Search Results tab. You can select the required devices from the Search Results tab. The Selection tab reflects whatever you selected from Search Results.

If you click the All tab now, the devices selected from Search Results will be shown in the All Devices group.

Selection Combining All and Search

After you select devices using the All tab, you can add a few more devices using Search. You can enter the search criteria and search using Search or Advanced Search and the Search Results tab displays the devices matching the criteria.

You can select the required devices from the Search Results tab. The Selection tab displays the accumulated list from both All and Search Results tabs. If you click the All tab, it displays the selected devices from Search Results under the All Devices group also.

You can enter another search criteria and select more devices. The selected devices are accumulated in the All tab from the Selection tab, as you select more devices.

Note The (n) Devices Selected message at the bottom left of the Device Selector screen shows the number of devices you have selected. It launches the Selection tab when you click on it.

Device Icons and Device Types

This section lists all CiscoWorks device icons mapped to the CiscoWorks device types See Table 3-14:

Table 3-14 Device Icons Mapped to Device Types

Device Icon	Device Type	Device Type Example (This list is not comprehensive and only has samples)
	Universal Gateways and Access Servers	• Cisco AS5300 Universal Gateways • Cisco AS5400 Series Universal Gateways • Cisco AS5800 Universal Gateways • Cisco AS5X00 Series Access Servers • Cisco 2500 Series Access Servers • [and so on]
	Cisco AS5200 Series Universal Access Servers	• AS5200 • [and so on]
	Content Networking	• Cisco Content Service Switch (CSS) 11000 Series • Cisco Content Service Switch (CSS) 11000 Series • Content Engine-500 Series • [and so on]
	Cisco Distributed Director	• Content Distribution Manager Series (CDM-4630, CDM-4650) • [and so on]
	DSL and Long Reach Ethernet (LRE)	• Cisco DSL Switches (6015 IP DSL, 6160 IP DSL, 6260 IP DSL) • Catalyst 2900XL Series (2924 LRE XL, 2912 LRE XL) • [and so on]
	Optical Networking	• Cisco ONS Series (ONS 15540 ESP, ONS 15530 ETSI) • [and so on]

Table 3-14 Device Icons Mapped to Device Types (continued)

Device Icon	Device Type	Device Type Example (This list is not comprehensive and only has samples)
	Routers	• Cisco 7500 Series • Cisco 3700 Series • Cisco 2500 Series • Cisco 1700 Series • [and so on]
	Switches and Hubs	• Catalyst 6000 Series • Catalyst 4000 Series • Catalyst 3900 Series • FastHub (300, 316T, 3116) • [and so on]
	Cisco 1538 Series Micro Hubs	• MicroHub(1502, 1503, 1516) • [and so on]
	Cisco Catalyst 5500 Series Switches	• Catalyst 5500 • Catalyst 5505 • Catalyst 5509 • [and so on]
	Cisco BPX 8600 Series Switches	• BPX 8620 • BPX 8650 • [and so on]
	Cisco MGX 8200 Series Edge Concentrators	• MGX 8220 • MGX 8850 • [and so on]
	Security and VPN	• Cisco VPN 3000 (C3005, C3015, C3030) • PIX Firewall (515, 520) • [and so on]
	Broadband Cable	• Universal Broadband Routers (UBR) 7100 Series (7111, 7114) • Universal Broadband Routers (UBR) 900 Series (904, 905) • [and so on]
	Storage Networking	• Cisco Storage Switch (MDS9509, MDS9216) • [and so on]

Table 3-14 Device Icons Mapped to Device Types (continued)

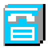
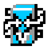
Device Icon	Device Type	Device Type Example (This list is not comprehensive and only has samples)
	Voice and Telephony	Any Cisco switch or router that is voice enabled (contains a voice card or voice port and its function is to aid IP Telephony operations). • Switch or router with FXS/FXO/T1/E1 interfaces. Routers with gatekeeper functions. • Cisco 1700 • Cisco 2600 • Cisco 3600 • [and so on]
	Cisco 7800 Series Media Convergence Servers	• Cisco 7845 Media Convergence Server • Cisco 7835 Media Convergence Server • Cisco 7830 Media Convergence Server • [and so on]
	Cisco VG200 Series Gateways	• VG224 • [and so on]
	Network Management	• CiscoWorks Wireless LAN Solution Engine • Cisco SwitchProbes • [and so on]
	CiscoWorks Hosting Solution Engine	• CiscoWorks 1105 Hosting Solution Engine, 1.3 • CiscoWorks 1105 Hosting Solution Engine, 1.4 • CiscoWorks 1105 Hosting Solution Engine, 1.5 • [and so on]
	Wireless	• Cisco Aironet AP Series (340, 350) • [and so on]
	Cisco Interfaces and Modules	• Catalyst 6000 modules (WS-SVC-IPSEC-1) • [and so on]

Table 3-14 Device Icons Mapped to Device Types (continued)

Device Icon	Device Type	Device Type Example (This list is not comprehensive and only has samples)
	Cisco Catalyst 6500 Series Network Analysis Module (NAM-1,2)	• Network Analysis Module • Network Analysis Module 1 • Network Analysis Module 2 • [and so on]
?	Unknown	Unknown device type.

Note

- To know more about Device Selector, refer to Common Services Online Help. See "Related Documentation" section on page -xxxiii
- The recommended number of devices for Contract Connection and Bug Tool Kit is 500. For Software Management (SWIM), the recommended number of devices is 1500. The recommended number of devices for rest of the modules in RME is based on the number of devices supported by each LMS 3.0 license. For more information on the number of devices supported by each LMS 3.0 license, see Installing and *Getting Started with CiscoWorks LAN Management Solution 3.0*

CHAPTER 4

Managing RME Device Groups Using Group Administration

Grouping devices and working with groups provides convenience to you in selecting required devices. You can define several groups of devices based on a set of criteria and manage the same. Device grouping provides an easy way of selecting the required devices.

There are two types of groups:

- System-defined Groups—The default grouping of devices in RME. This is a read only group. You cannot create groups under System-defined Groups. See Types of RME System-defined Groups.
- User-defined Group—Groups that you create to reflect the way you manage the network. You can create user-defined groups for RME (but not for Common Services).

  The User-defined groups can be either dynamic or static groups with private or public access privileges. You can also create subgroups under groups. Hence, each child group is a subgroup of a parent group.

RME manages groups in a hierarchical fashion that supports sub-grouping. Each child group is a subgroup of a parent group; in order to belong to a child group, a device must belong to the parent group. For an device to belong to a group, it must satisfy the child group rules and the parent group rules.

The features of grouping services are:

- The application groups are created by their respective grouping services.

  For example, RME groups are created by RME Grouping Services.
- The devices added to the applications are evaluated according to their respective group rules.

  For example, devices added to the RME are listed in appropriate device group based on the RME group rules.
- Based on the applications that are installed on the CiscoWorks server, you can view other applications' System-defined groups in RME user interface. The other applications User-defined groups are displayed in the RME user interface based on the Visibility Scope (public or private) for the group that you define at the time of device group creation.

  For example, you can view DFM System-defined groups in RME device selector.
- Based on the applications that are installed on the CiscoWorks server, you can view other applications' System-defined groups in RME user interface. However, only the RME devices are listed in the other application's System-defined groups.

  For example, you can view only RME devices in the DFM System-defined groups.

Types of RME System-defined Groups

The available RME System Groups are:

- All Devices—Contains all devices in RME. This a dynamic read-only group.
- Normal Devices—Contains all devices that have been successfully contacted by RME or the device has contacted RME at least once (Inventory polling, successful job completion, Syslog receipt etc.). This indicates that this is a real device in the network (at one point in time). This a dynamic read-only group.
- Pre-deployed—Contains all devices that are not reachable by RME. This a dynamic read-only group.
- Previous selection—Contains devices that are selected in previous RME task in the same session. This group is provided for your convenience in case you need to do different RME tasks on same set of devices. This a static read-only group.
- Saved device list—Contains all devices that are saved explicitly by you while generating the Inventory Reports (**Reports > Generator**). This group is provided for your convenience in case you need to do different RME tasks on same set of devices. This a static read-only group.

The Previous selection and Saved device groups are RME-specific groups and must be used only when you are working on a RME application. You cannot use these device groups when you are working on another CiscoWorks application. That is, if you are working on the Campus Manager application, these groups must not be used.

See Understanding the RME Device States for more details to understand how the devices are grouped based on RME System-defined rules.

Using RME Group Administration

The Group Administration page is where all group management activities take place. To open the Group Administration page from RME, select **Devices > Group Administration**.

The RME Group Administration window (Table 4-1) contains these fields:

Table 4-1 Fields on Group Administration and Configuration Page

Field/Button	Description
Group Selector	A hierarchical display of all available groups.
Group Info	When you select an item from the Group Selector, the Group Info pane displays the following information: • Group Name—The name of the group you selected. • Type—The type of objects in the selected group. • Description—A text description of the group. • Created By—The person who created the group. • Last Modified By—The last person to modify the group settings.
Create	Starts the Group Creation Wizard for creating a group, as described in the Creating a User-defined Group.
Edit	Starts the Group Edit Wizard for editing an existing group, as described in the Editing a User-defined Group.
Details	Opens the Properties: Details page, as described in the Viewing Group Details and Viewing Membership Details.

Table 4-1 Fields on Group Administration and Configuration Page (continued)

Field/Button	Description
Refresh	Refreshes a group's membership, as described in the Refreshing Membership.
Delete	Deletes a group, as described in the Deleting Groups.

Creating a User-defined Group

Creating an User-defined Group involves the four steps:

1. Entering the Group Properties Details in Properties: Create Dialog Box
2. Defining the Group Rules in the Rules: Create Dialog Box
3. Assigning Group Membership in the Membership: Create Dialog Box
4. Understanding the Summary: Create Dialog Box

You must complete all the four tasks in this sequence to create a group. If you exit the wizard at any stage using **Cancel**, the details you have specified will be lost and the group will not be created.

Entering the Group Properties Details in Properties: Create Dialog Box

In this step, you will enter the properties such as name and description, and modify the parent group and membership update method, if required.

The Properties:Create Dialog box contains the following fields:

Table 4-2 Create Dialog

Field	Description
Group Name	Name of the group you are creating.
Copy Attributes from Group	Copy the attributes of an existing group to your new group using the button Select Group. You can select either RME System-defined or User-defined groups.
Parent Group	The parent group of the group you are creating. You can change the parent group using the button Change Parent. You can select only RME User-defined groups.
Description	A text description of the group.
Membership Update	How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).
Visibility Scope	Describes if the group is visible for public (all users) or private (only for the group owner).

To enter the values in Properties:Create dialog box:

Step 1 Select **Resource Manager Essentials > Devices > Group Administration**.

The Group Administration and Configuration dialog box appears. This dialog box contains two panes.

- Group Selector—Lists all the System-defined Group and User-defined Group.
- Group Info—Contains the device group description.

Step 2 Select a User Defined Groups under which you want to create a new group from the Group Selector pane.

The Group Info pane displays detail of the selected user defined group.

The group that you have selected is the parent group for the new group you are about to create. You can change the parent group later, if required (see for changing the parent).

Step 3 Click **Create**.

The Properties:Create dialog box appears.

Step 4 Enter a name for the group in Group Name field of the Properties:Create dialog box.

The Group Name must be unique within the parent group. However, you can specify the same name in some other groups.

For example, if you already have a group named 'MyGroup' in a group named Views under User Defined Groups, you cannot use the same name for another sub-group in the group Views. However, you can use the name 'MyGroup' for the sub- group of another group in User Defined Groups.

If you do not want to copy the attributes of an existing group to your new group, proceed to Step 5. If you want to copy the attributes of an existing group to the new group, do the following:

All attributes except the group name are copied to the new group.

a. Click **Select Group**.

The Replicate Attributes dialog box appears.

b. Select a group.

You can select either RME System-defined or RME User-defined groups.

c. Click **OK**.

The parent group you have selected for the group does not change even if you are copying attributes from a group that belongs to a different parent group.

To change the parent group, do the following:

a. Click **Change Parent**.

The Select Parent dialog box appears.

b. Select the group.

Note You can select only RME User-defined groups.

c. Click **OK**.

The RME Group Administration changes the parent group to the one you selected, and returns to the Properties:Create dialog box.

Step 5 Enter a description for the group.

Step 6 Select the Membership Update mode for the group:

- Automatic (Dynamic)—The membership of the group is recomputed each time the group is invoked.
- Only upon user request (Static)—The membership of the group is recomputed only when an explicit request is made, using the Refresh option (**Resource Manager Essentials > Devices > Group Administration**).

Step 7 Select the Visibility Scope for the group:

- Private
- Public

Step 8 Click **Next**.

The Rules:Create dialog box appears.

Defining the Group Rules in the Rules: Create Dialog Box

In this step, you will define the rules for the group. The rules you define in this phase determine the contents of the group. The rules you specify here determine the devices to be included in the group.

If you have created the group copying the attributes of another group, the rules specified for that group appears in the Rule Text field. You can retain these and add more rules, or delete these rules and create a new set of rules.

Note All rules assigned to a parent group also apply to any of its subgroups.

In the Rules:Create dialog box, you can either enter the rules directly in the Rule Text field, or select the components of the rule from the Rule Expression fields, and form a rule.

The Rules:Create dialog box has the following fields:

Table 4-3 Rule Create Dialog box

Field/Buttons	Description
OR, AND, EXCLUDE	Logical operators. • OR—Include objects that fulfill the requirements of either rule. • AND—Include only objects that fulfill the requirements of both rules. • EXCLUDE—Do not include these objects. This field appears only after a rule expression is added in the Rule Text box.
Object Type	The type of object (device) that is used to form a group. All RME rule expressions begin with the same Object Type, RME:INVENTORY:Device.
Variable	Device attributes, based on which you can define the group. See Table 4-6Group Attributes.
Operator	The operator to be used in the rule. The list of possible operators changes based on the Variable selected. When using the *equals* operator the rule is case-sensitive.

Field/Buttons	Description
Value	The value of the rule expression. The possible values depend upon the variable and operator selected. Depending on the operator selected, the value may be free-form text or a list of values. The wildcard characters are not supported.
Add Rule Expression	Used to add the rule expression to the group rules.
Rule Text	Displays the rule.
Check Syntax	Verifies that the rule syntax is correct. Use this button if you have entered the rules manually.
View Parent Rules	Used to view the parent group rules. All parent group rules apply to the subgroups.

See Understanding the Grouping Rules for group rule restrictions and examples.

To create a new set of rules:

Step 1 Select the boolean operator field in the Rules:Create dialog box.

Step 2 Select the parameters for Object Type, Variable, and Operator.

Step 3 Enter the desired value for the Variable you have selected.

Step 4 Click **Add Rule Expression**.

The RME Group Administration creates the rule based on the parameters you specified and adds it to the rules already present in the Rules Text field. You can use the same procedure to add more rules.

You can manually add or change any of the text in the Rule Text box. If you enter a single backslash (\), an error is displayed. To enter a single backslash in the Rule Text box, you must type two backslashes (\\) in place of the single backslash. You should always check the syntax after changing a rule expression.

You can delete the rules displayed in the Rule Text field by selecting the complete rule expression.

For example, if the Rule expression is,

```
:RME:INVENTORY:Device.Chassis.Port_Count > "3" OR
```

If you want to delete a rule expression, you have to select the complete expression including the logical operator and press the delete key on your keyboard.

Step 5 Click **Check Syntax** to validate the rules expression syntax.

If the Syntax is correct, an information box appears with a message, The rule syntax is valid. If the Syntax is incorrect, an error box appears with syntax error messages along with the line and column number.

Step 6 Click **Next**.

The Membership:Create dialog box appears.

Assigning Group Membership in the Membership: Create Dialog Box

In this step, you will select devices to create a highly customized User Defined Group.

The RME Group Administration uses the details you have already specified while setting the group properties and group rules to decide the devices available to the group.

The Membership:Create dialog box contains two panes:

- Available Objects From Parent Group—Lists the devices that are available in the Parent Group.
- Objects Matching Membership Criteria—Lists the devices that match the membership criteria.

You can add or remove the devices from Objects Matching Membership Criteria list.

To add devices to the group:

Step 1 Select devices from Available Objects From Parent Group pane.

You can select multiple devices using Ctrl or Shift keys.

Step 2 Click **Add**.

The selected devices are removed from Available Objects From Parent Group pane to Objects Matching Membership Criteria pane.

Do not click the Refresh button on your browser after adding the devices. If you accidently do so, the device at the top of the Available Object From Parent Group pane gets added to list of the devices in the Objects Matching Membership Criteria pane.

Step 3 Click **Next**.

The Summary: Create dialog box appears with the group properties.

To remove devices to the group:

Step 1 Select devices from Objects Matching Membership Criteria pane.

You can select multiple devices using Ctrl or Shift keys.

Step 2 Click **Remove**.

The selected devices are removed from Objects Matching Membership Criteria pane to Available Objects From Parent Group pane.

Step 3 Click **Next**.

The Summary: Create dialog box appears with the User Defined Group properties.

Understanding the Summary: Create Dialog Box

The final step in the Create Group is a summary page that displays the new group's definition. The Summary: Create dialog box contains the following information:

Table 4-4 Summary Create Dialog box

Field	Description
Group Name	Name of the group you are creating.
Parent Group	The parent group of the group you are creating.
Description	A text description of the group.

Membership Update	How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).
Rules	The rules used to filter group membership.
Visibility Scope	Describes if the group is visible for public (all users) or private (only for the group owner).

After reviewing the group summary, either:

Step 1 Click **Finish** to complete the procedure for Creating Groups.

A confirmation box appears.

Step 2 Click **OK**.

You can view the newly created User Defined Group in the Group Selector pane.

Or

Click **Back** to change the group properties.

Editing a User-defined Group

You can edit all attributes that are defined while creating a group except for the *Parent Group* attribute.

The workflow for editing a User-defined group is:

1. Entering the Group Properties Details in Properties:Edit Dialog Box. You cannot modify the Parent Group.

See Entering the Group Properties Details in Properties: Create Dialog Box.

2. Defining the Group Rules in the Rules:Edit Dialog Box

See Defining the Group Rules in the Rules: Create Dialog Box.

3. Assigning Group Membership in the Membership:Edit Dialog Box

See Assigning Group Membership in the Membership: Create Dialog Box.

4. Understanding the Summary:Edit Dialog Box

See Understanding the Summary: Create Dialog Box.

You can click **Finish** at any point in the workflow.

Viewing Group Details

A group's information is displayed on the Properties: Details page.

Step 1 Select **Resource Manager Essentials > Devices > Group Administration**.

The Group Administration and Configuration dialog box appears.

Step 2 Select the group for which you want to view details from the Group Selector pane.

Step 3 Click **Details**.

The Properties: Details dialog box appears with the following information.

Table 4-5 Details Dialog box

Field/Button	Description
Group Name	Name of the group you are viewing.
Parent Group	Parent group of the group you are viewing.
Type	Type of the objects that belong to the group.
Description	Text description of the group.
Membership Update	How group membership is updated. Membership updates can be automatic (updated every time the group is accessed) or can be upon user request only (updated only when you click the Refresh button).
Created By	Person who created the group. This also displays the time when it was created.
Last Modified By	Last person to modify the group. This also displays the time when it was modified.
Rules	Rules used to filter group membership.
Visibility Scope	Describes if the group is visible for public (all users) or private (only for the group owner).
View Parent Rules This is a button.	Used to view the parent group rules. All parent group rules apply to the subgroups.
Membership Details This is a button.	Used to view the list of devices that belong to the group. See Viewing Membership Details.
Cancel	Closes the page and takes you back to the Group Administration and Configuration page.

Viewing Membership Details

You can view a list of the objects that belong to a group by accessing the Properties: Details page.

Step 1 Select **Resource Manager Essentials > Devices > Group Administration**.

The Group Administration and Configuration dialog box appears.

Step 2 Select the group for which you want to view details from the Group Selector pane.

Step 3 Click **Details**.

The Properties: Details dialog box appears.

Step 4 Click **Membership Details**.

The Membership Details dialog box appears with the following information.

Heading/Button	Description
Name	Name of the device.
Object Type	The type of object.
Property Details	Takes you back to the Properties: Details page.
Cancel	Closes the page and takes you back to the Group Administration and Configuration page.

Refreshing Membership

Refreshing a group's membership forces the group to recompute its membership by reevaluating its rules and obtaining membership information from the data collectors.

Step 1 Select **Resource Manager Essentials > Devices > Group Administration**.

The Group Administration and Configuration dialog box appears.

Step 2 Select the group for which you want to view details from the Group Selector pane.

Step 3 Click **Refresh**.

A confirmation dialog box dialog shows that the group membership will be recomputed.

Step 4 Click **Yes**.

A confirmation dialog box shows that the group membership is recomputed.

Step 5 Click **OK**.

Deleting Groups

You can only delete User-defined groups that are not one of the System-defined groups.

Step 1 Select **Resource Manager Essentials > Devices > Group Administration**.

The Group Administration and Configuration dialog box appears.

Step 2 Select the group for which you want to view details from the Group Selector pane.

Step 3 Click **Delete**.

A confirmation dialog box shows that the group will be deleted.

Step 4 Click **OK**.

Understanding the Grouping Rules

Every group is defined by a set of rules. A rule set contains a Boolean combination of individual rule expressions.

Rules are created to filter in the devices that you want to include to the group, and to filter out those that you do not want in the group.

When determining which devices belong to a group, Group Management compares device information to the rule. If the information on a device satisfies all the requirements of the rule then it is placed in the group.

The devices are filtered based on the data present in the RME Inventory database.

One or more rule expressions can be applied to form a rule.

Each rule expression contains the following:

`<object type>.<variable> <operator> <value>`

For examples on creating rules, see Examples for Grouping Rules.

Field/Buttons	**Description**
OR, AND, EXCLUDE	Logical operators. • OR—Include objects that fulfill the requirements of either rule. • AND—Include only objects that fulfill the requirements of both rules. • EXCLUDE—Do not include these objects. This field appears only after a rule expression is added in the Rule Text box.
Object Type	The type of object (device) that is used to form a group. All RME rule expressions begin with the same Object Type, :Device.
Variable	Device attributes, based on which you can define the group. SeeRME Group Attributes
Operator	The operator to be used in the rule. The list of possible operators changes based on the Variable selected. When using the *equals* operator the rule is case-sensitive.
Value	The value of the rule expression. The possible values depend upon the variable and operator selected. Depending on the operator selected, the value may be free-form text or a list of values. The wildcard characters are not supported.
Add Rule Expression	Used to add the rule expression to the group rules.
Rule Text	Displays the rule.
Check Syntax	Verifies that the rule syntax is correct. Use this button to verify the syntax of the rule created before proceeding to the next step.
View Parent Rules	Used to view the parent group rules. All parent group rules apply to the subgroups.

RME Group Attributes

The following table lists the available group attributes that you can use for defining the User Defined groups.

Table 4-6 Group Attributes

Attribute Group	Attribute Type	Description
Asset	Asset.CLE_Identifier	CLE identifier of the asset.
	Asset.Part_Number	Orderable part number of the asset.
	Asset.User_Defined_Identifier	User-defined identifier of the asset
Chassis	Chassis.Model_Name	Name of the model.
	Chassis.Number_Of_Slots	Number of slots in that chassis.
	Chassis.Port_Count	Total port count of the chassis.
	Chassis.Serial_Number	Serial number of the chassis.
	Chassis.Vendor_Type	Type of vendor for the chassis.
	Chassis.Version	Version number of the chassis.
Flash	Flash.File_Name	Location of flash file.
	Flash.File_Size	Flash file size in MB.
	Flash.Model_Name	Model name of the flash device.
	Flash.Partition_Free	Free space in MB.
	Flash.Partition_Name	Flash partition name.
	Flash.Partition_Size	Flash partition size in MB.
	Flash.Size	Total flash device size in MB.
Image	Image.ROM_Sys_Version	System ROM software version
	Image.ROM_Version	Version of ROM.
	Image.Sys_Description	Image system description
	Image.Version	Running Device image version.
IP Address	IP.Address	Device IP address.
	IP.Address_Type	Version of IP, IPv4 or IPv6
	IP.Network_Mask	Network Mask address
Memory	Memory.Free	Free memory in MB.
	Memory.Name	Name of the memory.
	Memory.Size	Total RAM size in MB.
	Memory.Type	Memory type.
	Memory.Used	Used memory in MB.
Module	Module.HW_Version	Module hardware version.
	Module.Model_Name	Name of the model.
	Module.Port_Count	Total ports on that module.
	Module.Serail_Number	Serial number of the module.
	Module.Vendor_Type	Type of vendor for the module.

Attribute Group	Attribute Type	Description
Processor	Processor.Model_Name	Name of the model.
	Processor.NVRAM_Size	Size of the processor NVRAM in MB.
	Processor.NVRAM_Used	Size of the processor NVRAM that has been utilized, in MB.
	Processor.Port_Count	Total port count of the processor
	Processor.RAM_Size	Size of the processor RAM in MB.
	Processor.Serial_Number	Serial number of the processor.
	Processor.Vendor_Type	Type of vendor for the processor.
State	State	RME device state such as Normal, Alias, etc.
System	System.Contact	Device contact person name.
	System.Description	Description of the system.
	System.DomainName	Device domain name.
	System.Location	Device location information.
	System.SystemOID	System Object ID of the device (sysObjectID).

Examples for Grouping Rules

Rule to select all the devices in Pending state

This rule filters all devices in Pending state.

To provide rule expression for this scenario:

From the Create Rules dialog box:

- Select **Device** from the Object Type drop down listbox
- Select **State** from the Variable drop down listbox
- Select **=** from the Operator drop down listbox
- Select **Pending** from the Value drop down listbox
- Click **Add Rule Expression**

The following rule gets added to the Rule Text:

```
Device.State = "Pending"
```

Rule to select devices whose System Description contains the string: Cisco Internetwork Operating System

This rule filters all devices whose System description consists of the string Cisco Internetwork Operating System.

To provide rule expression for this scenario:

From the Create Rules dialog box:

- Select **Device** from the Object Type drop down listbox
- Select **System.Description** from the Variable drop down listbox
- Select **contains** from the Operator drop down listbox

- Enter **Cisco Internetwork Operating System** in the Value textbox
- Click **Add Rule Expression**

The following rule gets added to the Rule Text:

```
Device.System.Description contains "Cisco Internetwork Operating System"
```

Rule to select devices whose contact person name consists of the word: Davis

This rule filters all devices whose contact person name consists of the word Davis.

To provide rule expression for this scenario:

From the Create Rules dialog box:

- Select **Device** from the Object Type drop down listbox
- Select **System.Contact** from the Variable drop down listbox
- Select **contains** from the Operator drop down listbox
- Enter **Davis** in the Value textbox
- Click **Add Rule Expression**

The following rule gets added to the Rule Text:

```
Device.System.Contact equals "Davis"
```

Rule to select devices whose location name equals: San Jose

This rule filters all devices whose location equals to San Jose.

To provide rule expression for this scenario:

From the Create Rules dialog box:

- Select **Device** from the Object Type drop down listbox
- Select **System.Location** from the Variable drop down listbox
- Select **equals** from the Operator drop down listbox
- Enter **San Jose** in the Value textbox
- Click **Add Rule Expression**

The following rule gets added to the Rule Text:

```
Device.System.Location equals "San Jose"
```

Rule with OR Operator

Rule to list all devices in normal state and/or the devices whose domain names contain the word cisco.

To provide rule expression for this scenario:

1. From the Create Rules dialog box:
   - Select **Device** from the Object Type drop down listbox
   - Select **State** from the Variable drop down listbox
   - Select **=** from the Operator drop down listbox
   - Select **Normal** from the Value drop down listbox
   - Click **Add Rule Expression** button

   The following rule gets added to the Rule Text:

   ```
   Device.State = "Normal"
   ```

2. Select the **OR** option from the logical operator list box.
3. From the Create Rules dialog box:
    - Select **Device** from the Object Type drop down listbox
    - Select **System.DomainName** from the Variable drop down listbox
    - Select **contains** from the Operator drop down listbox
    - Enter **cisco** in the Value textbox
    - Click **Add Rule Expression** button

   The following rule gets appended to the Rule Text:

   ```
   Device.State = "Pending" OR
   ```

   ```
   Device.System.DomainName contains "cisco"
   ```

The OR logical operator evaluates if either or both of the conditions are satisfied. The devices are selected based on either or both of the matching criteria.

Rule with AND Operator

Rule to list all the devices in Normal state with occurences of 1.3.6.1.4.1.9.1 in the System Object ID.

To provide rule expression for this scenario:

1. From the Create Rules dialog box:
    - Select **Device** from the Object Type drop down listbox
    - Select **State** from the Variable drop down listbox
    - Select **=** from the Operator drop down listbox
    - Select **Normal** from the Value drop down listbox
    - Click **Add Rule Expression**

   The following rule gets added to the Rule Text:

   ```
   Device.State = "Normal"
   ```

2. Select the **AND** option from the logical operator list box.
3. From the Create Rules dialog box:
    - Select **Device** from the Object Type drop down listbox
    - Select **System.SystemOID** from the Variable drop down listbox
    - Select **contains** from the Operator drop down listbox
    - Enter **1.3.6.1.4.1.9.1** in the Value textbox
    - Click **Add Rule Expression**

   The following rule gets appended to the Rule Text:

   ```
   Device.State = "Normal" AND
   ```

   ```
   Device.System.SystemOID contains "1.3.6.1.4.1.9.1"
   ```

The AND logical operator evaluates if both the criterias are satisfied. Only devices that satisfy both the criteria are selected.

Note Use Group Administration under Common Services (**Common Services** > **Groups** > **Group Admin**), to create groups with other device attributes like displayname, user defined attributes, management address in DCR. For more information refer to Common Services Online Help.

RME Group Administration Process

The RME Group Administration depends on the *RMEOGSServer* process. If this process is not running, then an error message appears:

```
Error in communicating with Group Administration Server.

It may be down or not yet up. Please make sure that the Group Administration Server is
up and running, then refresh the page.
```

You can resolve this error by starting the *RMEOGSServer* process.

You can start this process using **Common Services > Server > Admin > Processes.** In the Process Management page**,** select the *RMEOGSServer* and click **Start**.

CHAPTER 5

Understanding RME Device State Transition

The device participation in RME application tasks is no longer dependent on the device being in the Managed State as in RME 3.x. Instead, it will depend upon the actual device information required by the application task.

This allows RME to become flexible in meeting requirements to perform tasks on devices that have not yet been installed on the network.

Examples of such use-cases are pre-provisioning devices, managing spares, asset tracking, etc.

This section describes:

- The old State Management Behavior.
- The new State Management Architecture. These states are visible to you using the RME Device Management GUI.
- Examples of RME Application Tasks with description of the device information required for the task.

RME 3.x Behavior

In RME 3.x, devices that were added by you to RME could fall into one of the following states:

- Managed—All inventory data for the device was collected from the device. Application tasks were initiated only on devices in this state, and you could only see these Managed devices in the device selector.
- Suspended—You have explicitly barred these devices from being included in Application tasks. These devices will not be seen in the device selector.
- Not Responding—When the device was added, Inventory data could not be collected for the device either because the device was unreachable or the credentials to access the device were incorrect. You have to correct any errors and manually resubmit the device for management.
- Aliased Devices—If the duplicate detection module in RME finds that this added device is a duplicate of an already managed device, this device is put into the Aliased state.
- Conflicting State—When the devices were added, a new device might have the same name as an already managed device but differences in one or more device passwords. A conflict might be found, for example, in the Read or Write community strings, Telnet password, or console-enable password.

Only devices in the managed state can be selected from the device selector for application tasks. Also, automated actions are taken only on Syslogs from managed devices. Most Syslog reports are also restricted to this set of devices.

Thus, in RME 3.x, a device had to be in managed state for most application tasks. However, some application tasks allowed devices that were not in the managed state. They were:

- Import Status Report—Displays the number of devices in the various RME 3.x states.
- Syslog Unexpected Device Report—Displays a list of Syslogs received from devices that are not in RME 3.x managed state.

States in RME 4.x

The following describes the states a device can be in, and some sample application scenarios to explain the state.

The device states in RME, visible to all application are:

- Normal—Device has been successfully contacted by RME or the device has contacted RME at least once (polling, successful job completion, Syslog receipt etc.). This indicates that this is a real device in the network (at one point in time). Only the user can move a device out of this state.

  This state does not guarantee that there was a successful Inventory Collection. Also note that the Pre-deployed and Normal states are meant primarily for the information of the end-user.

  As in the Pre-deployed state, RME should allow/disallow application tasks purely based upon the presence/absence of the information required for that task.

  In the device selector, devices in the normal state will appear in the appropriate MDF –based groups, and in custom groups, if the data necessary to resolve group membership is available.

  Application tasks initiation and execution will behave exactly as described for devices in the pre-deployed state.

- Pre-deployed—Device has never been contacted by RME by any protocol (SNMP, SSH, etc.). Any successful contact with the device (be it SNMP polling, pre-provisioned job completion, etc.) will take it out of this state and into the Normal State.

  This state helps you to identify the devices that are to be deployed. These devices will appear in the device selector in a separate group, Pre-deployed. These devices also appear under the appropriate MDF-based groups, based on the information entered in DCR.

  The operator can initiate application tasks (includes jobs) using devices in this state by using the device selector in the same way as Normal devices.

  However, some application tasks may not execute or be scheduled, since the information required for that task is not yet available in RME.

  Thus, Software Managemente’s Distribution Method by devices [Advanced] flow job creation task succeeds, since there is no data required from the device either current or cached.

  On the other hand, Software Management Device Centric job creation task that requires Image Recommendation fails since the required Flash and Image data is not yet available in RME.

  Application tasks will succeed or fail on a best-effort basis without depending on whether there is a full Inventory Collection performed on the device.

  RME will have inventory and Configuration polling and collection jobs for all devices in the pre-deployed state. If any of these jobs successfully contact the device, the device is moved to Normal state.

- Pending—This is a transient state, and, in an operational RME, no device will be in this state for any significant time.

These devices appear in the device selector in a separate group, Pending. The operator can initiate application tasks (including jobs) by selecting these devices from the device selector.

When the device is added to RME, device management puts the device into this state, and invokes all the registered application tasks such as Inventory Collection, Configuration collection, etc. Based on the results of the tasks, the device goes into Pre-deployed, Normal or Aliased states.

- Suspended—You may suspend a device because you do not want to manage it, have it participate in any RME application tasks. Only you can move a device out of this state. RME application does not allow devices in this state to participate in normal RME application tasks (except for special cases like the Suspended Device Report).

  Suspended devices do not appear in the device selector. Syslogs from these devices do not cause any automated actions to happen. However, syslogs from devices in this state are collected and reported on.

- Aliased—Devices that have been detected as duplicates, at the time of Device Addition, as done in RME 3.x. These devices cannot participate in RME application tasks (except for special cases like the Duplicate Device Report).

  These states are visible to you in the Device Management GUI and the Device Summary Report. Here you can see how many devices are in each of the states.

  There is a report that allows you to select a set of devices and view the states that they are in.

- Conflicting State—Devices that have the same name/IP Address as an already managed device, but the sysObjectID for the two conflict. The user has to resolve this conflict. Note that the already managed device continues to be in the managed state, and participates in all application tasks. The new entry with conflicting credentials will go to the conflicting state.

  These states will be made visible to the user via the Device Management GUI and the device summary report to allow the user to see how many devices are in each of the states.

State Transitions

The following defines how the state of a device can change in RME 4.1

- Pending
- Pre-deployed
- Normal
- Aliased
- Suspended
- Conflicting

Pending

The Pending state occurs:

- If Inventory Collection for the device has succeeded, and the alias detection algorithm has determined that this device is an alias of a device that is already in the Normal state, the device is moved to the Aliased state requiring user interaction.
- If History for the device exists, the device is directly moved from pending to normal state, without waiting for the results of the registered tasks.

- If there is no history for the device, tasks registered with Device Management (such as Inventory Collection or Config Collection) for the device has succeeded in contacting the device.
- If Alias detection algorithm either determined this was not an alias of an existing device, or did not have sufficient information to make this decision, the device goes to the Normal state.
- If none of the tasks registered with Device Management were successful in contacting the device, the device goes to the Pre-deployed state.

Pre-deployed

The Pre-deployed state occurs:

- If any RME task succeeds in contacting the device, the device is moved to Normal state.
- If the operator picks the device in Pre-deployed state, and suspends it, the device moves to Suspended state.
- If the operator picks the device in Pre-deployed state and deletes it from RME, the device goes out of RME.

Normal

This is a rare case:

For example if device d1 and d2 are aliases, d1 is added to RME, goes to pre-deployed state. The device d2 also goes into pre-deployed state. RME does not know that they are aliased. The d1 and d2 devices are in separate jobs.

When job j1 runs, d1 is contacted and moves to Normal state. RME still does not know that d2 is an alias. Now, job j2 runs on d2 device, and d2 device is moved to Normal state. Now alias detection should catch that d1 and d2 are aliases, and should move d2 to Aliased state from Normal state.

- If the operator picks the device in Normal state and deletes it from RME, the device goes out of RME
- If the operator picks the device in Normal state, and suspends it, the device moves to Suspended state

Aliased

The Aliased state occurs:

- If the user manually re-submits the device for RME management, the device goes to the Pending state.
- If the operator picks the device in Aliased state and deletes it from RME, the device goes out of RME

Suspended

The Suspended state occurs:

- If the operator picks the device in Suspended state and deletes it from RME, the device goes out of RME.
- If the user manually re-submits the device for RME management, the device goes to Pending state.

Conflicting

The Conflicting state occurs:

- If the operator picks the device in Conflicting state and deletes it from RME, the device goes out of RME.
- If the user manually updates the device credentials for RME management, the device goes to Pending state.

RME 4.x Scenarios

The following section describes the RME 4.x scenarios:

- Device Addition
- Inventory Detailed Device Report
- Configuration Deployment Using Config Editor
- Configuration Changes Using NetConfig
- Software Image Upgrade

Device Addition

This describes the application task where RME does not have the automatic synchronization with Device and Credential Repository (DCR) enabled.

1. Operator adds one or more devices to DCR, providing all the required attributes and credentials.

   The mandatory fields from DCR are:

   a. Management IP address or Host Name or Device ID, Display Name.
   b. Device MDF category or SysObjectID is expected to be valid value for the Device Type field. This is required to instantiate the correct device package for RME jobs (for example, NetConfig job creation).
2. DCR informs RME that new devices have been added, and RME updates its picker list.
3. Operator selects devices from the picker list to add to RME.

   For each selected device, Device Management puts the device into pending state. It then invokes the registered RME application tasks such as Inventory Collection, Config Collection etc.

   - If no task succeeds in contacting the device, the device is put into the Pre-deployed state by Device Management.
   - If RME's alias detection is successful and finds that this device is a duplicate of an existing device in either the Pre-deployed or Normal states, the new device is put into the Aliased state.
   - If alias detection does not mark this device as being Aliased (either because it did not have sufficient information to make the decision or the algorithm identifies the device to be unique)

     and
   - If any of the application tasks in step 4 succeed in contacting (exchanging any packets) with the device, the device is moved to the Normal state. Note that no application task has to succeed in order for this to happen – Contact is sufficient.
4. The device selector displays all devices that are in the Pending, Pre-deployed, and Normal states.

   The devices in Pre-deployed state appear in the system-defined MDF groups as well as a special group called Pre-deployed.

Similarly, devices in the pending state will also appear in the special group Pending as well as in the relevant locations in the MDF grouping. This helps you to quickly select all such devices for a specific task.

Device Management's Device Summary report displays the number of devices in each of the above states.

Note Inventory Collection and Inventory Polling will have a system defined periodic job that will operate on all devices in both the Pre-Deployed and the Normal states. The actual set of devices to be collected or polled on will be determined at the job execution time.

Inventory Detailed Device Report

The device selector for this task displays all devices in the Normal and Pre-Deployed states. You can select a set of devices for their detailed report. The application will use the application local states to determine the display format of the details for each device. Those devices that have no details collected at all will display `No Details Available`.

Reports for devices with partial data display this partial data in the appropriate locations.

Configuration Deployment Using Config Editor

To deploy a configuration using Config Editor, you need to:

Step 1 Select a Config file for editing.

Step 2 Edit the configuration file using either of the following options:

- **a.** Device and Version,
- **b.** Pattern Search
- **c.** Baseline
- **d.** External Location

Step 3 Click **Save** to save the file after editing it.

Step 4 Deploy a configuration by creating a deployment job, by selecting the recently saved configuration file.

To create a deployment job,

a. Select one or more devices from the Device Selector.

These selected devices could be in pending, pre-deployed or normal states. This task does not need any additional information from the Inventory DB (except for device type).

b. Set the download mode to either Merge or Diff if the device is in the normal state and at least one version of the configuration for the device has been archived.

Only merge mode is possible in the case of Pending or Pre-deployed devices or for those devices in the Normal state for which no configuration is archived yet.

The below table describes the various job options:

Job Options	Description
Different Configuration Versions Considered Failure	This requires at least one configuration version to be archived.
Sync Archive before Job execution	Applicable to devices in all of pending, Pre-deployed and Normal states. Failure to get the configuration at job execution time fails the job.
Write running to startup configuration	Applicable to devices in all Pending, Pre-Deployed and Normal States.

c. Provide the job policies and scheduling information.

d. Click on **Submit** button to submit the job.

At the scheduled time, the job is executed. For Job Execution there is no mandatory requirement for the existence of any inventory or Config Archive data.

Configuration Changes Using NetConfig

To make configuration changes using NetConfig:

Step 1 Select a set of devices from the device selector that contains all of Pending, Normal and Pre-deployed devices.

Step 2 Select a set of task types to be executed on these devices (Banner change, SNMP Credentials change etc.).

For each device type and task type selected, you must enter the relevant parameters.

If a particular task requires inventory data (for example, Cable templates that require Interface details) and if the required inventory data is not available, you will be prompted with a warning that the job cannot include that particular task.

Step 3 Select any of these options to continue creating a job:

- Different Configuration Versions Considered Failure—Requires at least one configuration version to be archived.
- Rollback failure policies—At job creation time, all the rollback policies for failure apply to devices in Pending, Pre-Deployed and Normal states.
- Sync Archive before Job execution—Applicable to devices in any of Pending, Pre-deployed and Normal states. Failure to get the Config at job execution time fails the job.
- Write running to startup configuration—Applicable to devices in any of Pending, Pre-Deployed and Normal States.

Step 4 Submit the job after selecting the job policies and entering the job scheduling information.

At the job execution time, before deploying the Config changes:

- If sync archive policy is selected, and if archival fails (at the time of execution) the job fails. (Current behavior).
- If rollback policy is selected, and no configuration has been collected for this device, the job execution will proceed with a warning in the job results.

- If the device is reachable: NetConfig attempts to fulfill the selected job options, and deploys the configuration to the device. If the device was in the Pre-deployed or Pending states, Device Management is informed that the device is now contactable.
- If the device not reachable: The configuration deployment to this device is marked as failed, and no state change is requested for.

Software Image Upgrade

To perform Image Distribution by Device (Advanced):

Step 1 Select the Image Distribution by Device (advanced) task. The inventory data is not required.

Step 2 Enter the image, target device and the target destination on the device. The devices can be in the Normal, Pending, or Pre-deployed states.

For each device Software Management attempts to get required data to do the verification.

Examples of the data required for this verification include the boot loader version for IOS devices, or the Version running on the supervisor for a Card to be upgraded, and physical attributes like free flash on the given partition.

The exhaustive data list is device type specific and will be provided in the Software Management design documents. This data is got from Inventory via ADI.

If verification is possible with the data for the device, Software Management does the verification and marks the device as verification passed or failed.

If there is insufficient data for this operation, Software Management marks the device as skipped due to insufficient data, however if the user had specified best-effort verification, the job gets scheduled for execution with the skipped devices included.

If you had chosen mandatory verification, job creation fails.

At execution time, Software Management attempts to contact each device.

- If the device is contactable, and Software Managemente’s internal checks work out, the image is downloaded to the device, and this device is marked as successful.
- If the device was in pending or pre-deployed states at the time of job execution, Software Management will inform Device Management that the device was contacted.
- If the device is not contactable at the job execution time, Software Management will mark this download as failed, and will continue on with the rest of the devices in the job. No state changes will be effected.

CHAPTER 6

Managing Inventory Collection and Polling Using Inventory

Inventory, or the Inventory Collection Service (ICS) and Poller software component of RME, collects inventory data from the network devices and keeps the inventory updated. It does this by:

- Enabling you to collect inventory periodically. You can ensure that inventory data is collected periodically to avoid the usage of stale inventory data by other RME applications.
- Polling the devices for any changes in inventory. If it detects a change, it invokes a full inventory data collection. The following poller AG variables are supported:
  - ifTableLastChange
  - ifLastChange
  - ifStackLastChange
  - entLastChangeTime
  - sysUpTimeAtLastChassisChange
  - ciscoFlashDeviceInitTime
  - ciscoLS1010ChassisLastChange
- Initiating inventory data collection on request.

  For example, when the Syslog application receives an inventory change Syslog message, it invokes inventory data collection using the API that Inventory registers with Syslog.

  RME acquires inventory data from devices using SNMP queries to standard SNMP MIB II objects and Cisco-specific enterprise MIB objects.

For the new features in this release, see What's New in this Release.

Note You can select the log level settings for the Inventory application using the feature Application Log Level Settings (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

How to Use Inventory

You can use the Inventory application of RME for:

- Collecting and Updating Inventory Data
- Viewing Reports and Graphs

Pre-requisites

Before you schedule inventory polling and collection jobs, you must:

Step 1 Add or import devices and add their credentials to the Device and Credentials Repository Administration (DCR) database.

Step 2 Add devices in RME using **Resource Manager Essentials > Devices > Device Management > RME Devices**.

In the RME Devices dialog box that appears, click **Add Devices**. For the detailed procedure, see the topic Adding Devices to RME in the section Adding and Troubleshooting Devices Using Device Management.

We also recommend that you enter the RME device attributes:

a. Select **Resource Manager Essentials > Devices > Device Management > RME Devices**.

   The RME Devices dialog box appears.

b. Select the devices for which you want to edit the RME device attributes and click **Edit Device Attributes.**

For more Device Management information, see the section Adding and Troubleshooting Devices Using Device Management in the User Guide or Online Help.

Note Any change that you make to the system time affects RME processes. You will have to restart the Daemon Manager for the proper functioning of RME.

You can select the log level settings for the Inventory application using the feature Application Log Level Settings.

Collecting and Updating Inventory Data

To ensure that your inventory data is up-to-date, use RME to:

- Schedule inventory collection. (A default job is created when you install RME, and you can change the schedule of this job as required.) For details see Creating and Editing an Inventory Collection or Polling Job.

  Schedule “heavyweight” collection of inventory data from all managed devices to run and update the database at regular intervals.

- Set inventory poller schedule. (A default job is created when you install RME, and you can change the schedule of this job as required.) For details see Creating and Editing an Inventory Collection or Polling Job.

  Schedule periodic polling to see if any changes have occurred on any managed devices, and, if changes are detected, trigger an inventory collection on only the changed devices.

- Create and run user-defined inventory collection jobs.
- Create and run jobs. You can schedule jobs on specific sets of devices to run immediately, once, or periodically, with a frequency such as 6- hourly, 12-hourly, daily, weekly or monthly.

  In this way, you can update your inventory database and show the changes in all the associated inventory reports. For details see Creating and Editing an Inventory Collection or Polling Job.

Before you run inventory collection see Pre-requisites.

View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform these tasks.

Inventory log files (IC_Server.log, ICServer.log, ICServerUI.log, and invreports.log) are stored at these locations:

- On Windows: *NMSROOT*/log, where *NMSROOT* is the CiscoWorks installation directory.
- On Solaris: /var/adm/CSCOpx/log

Viewing Reports and Graphs

You can monitor the system, interface, hardware, and software details of your network devices. Note that a history of inventory changes are logged by and viewed through Change Audit. Reports and graphs listed here are viewed from the Inventory application.

- 24-Hour Inventory Change Report (see Generating a 24 Hour Inventory Change Report).

  Shows the details of all inventory changes that were detected on the device during the last 24 hours.
- Chassis Slot Summary (see Generating a Chassis Slot Summary) and Chassis Slot Details (see Generating Chassis Slot Details).

  Shows overview and detailed capacity information for selected devices.
- Hardware Report (see Generating a Hardware Report) and Software Report (see Generating a Software Report).

  Shows summary of device hardware and software data. For example, you can run these reports before you perform a hardware or software upgrade to help determine the scope of the work involved.
- Generating a Detailed Device Report.

  Shows the details about all stored inventory data (hardware, flash, memory, software, etc.) for selected devices.
- Generating a PSIRT Summary Report.

  Provides a summary of the possible security alerts, based on the selected devices.
- Generating End of Sale/End of Life Report

  Provides a summary of the end of sale or end of life alerts, based on the selected devices.
- MultiService Port Details (see Generating MultiService Port Details).

  Shows details about a selected switch's multiservice ports that supply power while supporting voice traffic.
- Hardware Summary Graph (see Generating a Hardware Summary Graph).

  Shows the distribution of device types among all the managed device classes.
- Chassis Summary Graph (see Generating a Chassis Summary Graph).

  Shows the distribution of chassis types among all the managed device classes.
- Software Version Graph (see Generating a Software Version Graph).

  Shows the distribution of software versions among all the managed device classes.
- Inventory Custom Reports (see Using Inventory Custom Report Templates).

  Shows device details by their attributes, see Table 6-9, Table 6-9Inventory Groups and Attributes.

You can save the reports that you have generated, in a comma separated (CSV) format or in the PDF format. Redirect a report to an e-mail recipient, save the report, or run it again later.

Using the Inventory Job Browser and Viewing Inventory Collection Status

The Inventory option of Resource Manager Essentials (**Resource Manager Essentials > Inventory**), enables you to:

- Use the Inventory Browser (see Using the Inventory Job Browser).
- View the Inventory Collection status (see Viewing Inventory Collection Status).

Using the Inventory Job Browser

The Inventory Job Browser displays all user-defined jobs. It also displays the system-defined inventory collection and polling jobs. You can create and manage inventory jobs using the Job Browser. You can edit, stop, cancel or delete jobs using this Job Browser.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform these tasks.

When you install RME, a default job is defined for Inventory Collection and Inventory Polling.

These default jobs include all the devices in the normal and pending states, and the devices in the pre-deployed state.

When the default job runs, RME evaluates the “all devices” group and executes the job. This way whenever new devices are added to the system, these devices are also included in the default collection/polling job.

For the default system jobs, the device list cannot be edited. You can only change the schedule of those jobs. Therefore, when a periodic system job for inventory collection or polling is scheduled, the scheduled job is not displayed in the Inventory Job Browser.

The default system jobs for Inventory Collection and Inventory Polling are created immediately after installation. However, they may appear in the Inventory Job Browser and the RME Job Browser (**Resource Manager Essentials > Job Mgmt > RME Jobs**) only after some time has elapsed.

The jobs are displayed in the Job Browser when they are running, or after they are completed, with all the details such as Job ID, Job Type, Status, etc.

User-defined jobs, however, are displayed in the Job Browser once they are scheduled, when they are running, and after they are completed.

To invoke the Inventory Job Browser:

Select **Resource Manager Essentials > Devices > Inventory > Inventory Jobs**.

The Inventory Job Browser dialog box appears with a detailed list of all scheduled inventory jobs.

The columns in the Inventory Job Browser dialog box are:

Column	Description
Job ID	Unique ID assigned to the job by the system, when the job is created. Click on the hyperlink to view the Job details (see Viewing Job Details.) Periodic jobs such as 6-hourly, 12-hourly, Daily, Weekly and Monthly, have the job IDs that are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Job Type	Type of job—System Inventory Collection, System Inventory Polling, Inventory Collection and Inventory Polling.
Status	Status of the job—Scheduled, Successful, Failed, Cancelled, Stopped, Running, Missed Start. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. This count of failed devices is not displayed for jobs restored from RME 4.0.4 or lesser versions.
Description	Description of the job entered by the job creator. This is a mandatory field. Accepts alphanumeric values. The field is restricted to 256 characters.
Owner	Username of the job creator.
Scheduled at	Date and time at which the job was scheduled.
Completed at	Date and time at which the job was completed.
Schedule Type	Type of schedule for the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

Using the Filter by field in the Inventory Job Browser, you can filter the jobs displayed in the browser.

You can filter the jobs using any of the following criteria and clicking **Filter**:

Filter Criteria	Description
All	Select **All** to display all jobs in the Job Browser
Job ID	Select **Job ID** and enter the whole or the first part of the Job ID(s) that you want to display.

Filter Criteria	Description
Job Type	Select **Job Type** and then select any one of the following: • Inventory Polling • System Inventory Polling • Inventory Collection • System Inventory Collection
Status	Select **Status** and then select any one of these: • Schedule • Successful • Failed • Cancelled • Stopped • Running • Missed Start Missed start is the status when the job could not run for some reason at the scheduled time. For example, if the system was down when the job was scheduled to start, when the system comes up again, the job does not run. This is because the scheduled time for the job has elapsed. The status for the specified job will be displayed as `Missed Start`.
Description	Select **Description** and enter the first few letters or the complete description.
Owner	Select **Owner** and enter the user ID or the beginning of the user ID.
Schedule Type	Select the **Schedule Type** and select any one of these: • Immediate • Once • 6-hourly • 12-hourly • Daily • Weekly • Monthly

Refresh (Icon)	Click on this icon to refresh the Inventory Job Browser.

To perform the following tasks, use the Inventory Job Browser:

Table 6-1 .Inventory Job Browser Buttons, Tasks and Description

Button	Task	Description
Create	Create jobs	You can create a new job.
Edit	Edit jobs	You can edit a only a scheduled job. You can select only one job at a time for editing. If you select more than one job, the Edit button is disabled.
Cancel	Cancel jobs	You can cancel a scheduled job. You can select more than one scheduled job to cancel. You are prompted to confirm the cancellation. If it is a periodic job, you are prompted to confirm whether you want to cancel only the current instance of the job or all future instances. Select a periodic job and click **Cancel**. The Cancel Confirmation dialog box appears. 1. Select one of the following options: – Cancel only this instance – Cancel this and all future instances 2. Click **OK**.
Stop	Stop jobs	You can stop a running job. However, the job will be stopped only after the devices currently being processed are completed. This is to ensure that no device is left in an inconsistent state.
Delete	Delete jobs	You can delete a job that has been scheduled, successful, failed, stopped or cancelled. However, you cannot delete a running job. You can select more than one job to delete, provided they are scheduled, successful, failed, stopped, or cancelled jobs. For instance, if you select a failed job and a running job, the Delete button is disabled. If you are deleting a scheduled periodic inventory job, the following message is displayed: `If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must recreate the deleted jobs.` You are prompted to confirm the deletion.

Records for Inventory Collection and Polling jobs need to be purged periodically. You can schedule a default purge job for this purpose. See Job Purge in the section Setting System-wide Parameters Using System Preferences.

Viewing Job Details

In the Inventory Job Browser, click on the Job ID hyperlink to view the following job details for Inventory collection, or polling jobs:

- Job Details—Expand this node to display Job Summary and Job Results for the inventory collection or polling job.
- Job Summary—Click on this node to view the following for the inventory collection or polling job:
  - Job Summary—Displays information about the job type, the job owner, the status of the job, the start time, the end time and the schedule type.

  - Device Summary—Displays information about the total devices submitted for the job, the number of devices that were scanned, the number of devices that were pending, the devices that were successful with change, successful without change, and the failed devices.
- Job Results—Displays information about the number of devices scanned, the names of the scanned devices, the duration of scanning, the average scan time per device, and the job results description, for the inventory collection or polling job.

  To see more details, expand the Job Results node. You will see the following details:

  - Failed—If you click on this node, you will see the collective list of failed devices and the reason for their failure in the right pane, for the inventory collection or polling job.

    If you expand this node, the list of failed devices appears.

    If you select a device, the right pane displays the device name and the reason for the failure. For example, `Device sensed, but collection failed`, or `Device not reachable`.
  - Successful: With Changes

    For a Inventory collection job:

    Expand the Successful: With Changes node to display a list of devices.

    If you select a device, the right pane displays the device name and a hyperlink: View Changes. If you click on this hyperlink, the Inventory Change Details report appears for the device. The report displays information about the attribute, the type of change, the time of change, the previous value and the current value for the collection job.

    If you do not expand this node, you will see the collective list of devices with the status Success: With changes with their View Changes hyperlinks, in the right pane, for the collection job.

    There is a View All Changes hyperlink in the right pane. If you click this hyperlink, all the changes on the devices are displayed.

    For a Inventory polling job:

    Click on the Successful: With Changes node to display a list of devices that have changes, as a comma separated list, in your right pane. To view the Inventory collection job details for these devices, click the Inventory Collection Job Details hyperlink.
  - Successful: Without Changes

    If you click on this, you will see as a comma-separated list in your right pane, the devices that were successful for the inventory collection or polling job.

Note Inventory Poller creates a Collection job when it detects changes.

Creating and Editing an Inventory Collection or Polling Job

To create an Inventory collection or polling job:

Step 1 Go to the Inventory Job Browser and click **Create**. (To invoke the Inventory Job Browser, see Using the Inventory Job Browser).

The Create Inventory Job dialog box appears.

Step 2 Select either:

- Device Selector, if you want to schedule report generation for static set of devices (See the topic, Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management, for more details.) You can select devices that are in Normal, Pending or Pre-deployed states for job creation.

Or

- Group Selector, if you want to schedule report generation for dynamic group of devices.

Step 3 Enter the information required to create a job:

Field	Description
Job Type	Select either Inventory Collection or Inventory Polling, as required.
Scheduling	
Run Type	Specifies the type of schedule for the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. If you select Immediate, the date field option will be disabled.
Date	1. Enter the start date in the *dd Mmm yyyy* format, for example, 02 Jul 2004, or click on the calendar icon and select the date. 2. Enter the start time by selecting the hours and minutes from the drop-down list. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the report that you are scheduling. This is a mandatory field. Accepts alphanumeric values. This field is restricted to 256 characters.
E-mail	Enter e-mail addresses to which the job sends messages when the job has run. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address,

Step 4 Click **Submit**.

You get a notification that the job has been successfully created, and it appears in the Inventory Job Browser.

To edit a job, select a scheduled job from the Inventory Job Browser, and click **Edit**.

The Edit Inventory Job dialog box appears. The Job Type options are disabled. You can however, change the Scheduling and Job Info fields as required, and click **Submit**.

The job is edited.

Stopping, Cancelling or Deleting an Inventory Collection or Polling Job

You can stop, cancel or delete Inventory Collection or Polling jobs.

- Stopping a job, see Stop in Table 6-1.
- Cancelling a job, see Cancel in Table 6-1.
- Deleting a job, see Delete in Table 6-1.

Viewing Inventory Collection Status

You can view the status of Inventory collection.

Step 1 Select **Resource Manager Essentials > Inventory > View Inventory Collection Status**.

The Inventory Collection Status dialog box appears.

Step 2 View the Inventory collection status. SeeTable 6-2 for an example:

Table 6-2 An Example of Inventory Collection Status with Description

Inventory Collection Status	No. of Devices	Description
Inventory Collected	15	Click on the Devices hyperlink to view a report called Devices for which Inventory has been Collected at Least Once. The report displays the list of devices and the time of the last inventory collection, for each device. Click on the hyperlink for each device to view the details of that device, in Device Center.
Inventory Never Collected	10	Click on the Devices hyperlink to view the list of devices for which inventory has never been collected. Click on the hyperlink for each device to view the details of that device, in Device Center.
Inventory Recently Failed	15	Click on the Devices hyperlink to view a report called Devices for which Inventory has recently failed. The report displays the list of devices and the recent inventory collection failure time, for each device. Click on the hyperlink for each device to view the details of that device, in Device Center.
Total	25	Total number of devices for which the inventory collection status is displayed.

Refresh (Icon)	Click on this icon to refresh the Inventory Collection Status dialog box.

For more details about Device Center, see the CiscoWorks Common Services Online Help or User Guide.

Inventory Administrative Operations

Using the Admin tab of Resource Manager Essentials (**Resource Manager Essentials > Admin > Inventory**), you can perform the administrative operations for the Inventory application:

- Setting Change Report Filters.
- Changing the Schedule for System Inventory Collection or Polling.
- Cisco.com Fetch Interval

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform these tasks.

Setting Change Report Filters

Using the Inventory Change Filter dialog box, you can select the attributes that you do not wish to log using Change Audit. The history of inventory changes are logged by and viewed through Change Audit.

The attributes that you select in the Inventory Change Filter dialog box, are monitored for Inventory changes like other variables. However, they are not logged using Change Audit. Consequently, these changes are not displayed in your inventory change reports.

For example, for Stack devices, if you do not want to log the operational status for changes in Change Audit, select the Operational Status option in the Inventory Change Filter dialog box.

The Inventory Change Filter dialog box, displays each attribute group and the corresponding filters for the attribute group, for your selection.

- To view all inventory change reports, select **Resource Manager Essentials > Reports > Report Generator**. In the Report Generator dialog box, first select the application, Change Audit, and then select the Exception Period Report from the respective drop-down lists.
- To view inventory changes from the last 24 hours, select **Resource Manager Essentials > Reports > Report Generator**. In the Report Generator dialog box, first select the application, Inventory, and then select report 24 Hour Inventory Change report from the respective drop-down lists.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To set Inventory change filters:

Step 1 Select **Resource Manager Essentials > Admin > Inventory > Inventory Change Filter**.

The Inventory Change Filter dialog box appears.

Step 2 Select a group from the Select a Group drop-down list. See Table 6-3.

The dialog box refreshes to display the filters available for the attribute group that you selected.

Step 3 Select the attributes that you do not want to monitor for changes.

Step 4 Click **Save**.

A confirmation dialog box appears.

Step 5 Click **OK** to save the details.

You can use **Reset All** to reset your selections for *all* groups. This resets all previous values to blanks.

Table 6-3 Inventory Change Filters

Report Inventory Group	Custom Report Group/Attribute	Description
Asset	Orderable Part Number	Orderable part number of asset.
	Tag	Asset tag.
	CLE Identifier	Represents CLIE (Common Language Equipment Identifier) code for the physical entity.
	Mfg Assembly Revision	Manufacturing assembly revision of asset.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
	Mfg Assembly Number	Manufacturing assembly number of asset.
	Physical Index	Physical index of asset
Back Plane	Operational Status	Operational status of backplane.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Manufacturer Name	Name of manufacturer.
	Physical Entity Name	Name of physical entity.
	Slot Configuration	Configuration of backplane slots
	Model Name	Name of model.
	Vendor Type	Type of vendor.
	Serial Number	Serial number of backplane.
	Description	Description of backplane.
	Component Type	Type of component.
	Index	Index of backplane.
	Field Replaceable Unit	FRU of backplane. Field-replaceable unit is a hardware component that can be removed and replaced on site.
	Alias Name	Alias name of backplane.
Bridge	Bridge Type	Type of bridge.
	Number of Ports	Number of ports in the bridge.
	Base Bridge Address	Base address of bridge.
Chassis	Chassis Model Name	Name of the chassis model.
	Chassis Serial Number	Serial number of the chassis.
	Chassis Vendor Type	Type of vendor.
	Chassis Version	Version number of the chassis.
Chassis	Report Published	Indicates whether Report is published or not. Displays the value as True or False.
	Description	Description of chassis.
	Field Replaceable Unit	FRU of chassis.
	Component Type	Type of component.
	Alias Name	Alias name of chassis.
	Index	Physical index of chassis.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Physical Entity Name	Name of physical entity.
	Free Slots	Free slots in chassis.
	Slot Capacity	Slot capacity of chassis.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
	Operational Status	Operational status of chassis.
	Manufacturer Name	Name of manufacturer.
	Slot Configuration	Slot configuration of chassis.
Component	Index	Physical index of component.
	Field Replaceable Unit	FRU of component.
	Alias Name	Alias name of component.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Operational Status	Operational status of component.
	Manufacturer Name	Name of manufacturer.
	Name	Name of component.
	Slots Configured	Slot configuration of component.
	Model Name	Name of model.
	Vendor Type	Vendor type of component.
	Serial Number	Component serial number.
	Description	Description of component.
	Component Type	Type of component.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Container	Alias Name	Alias name of container.
	Operational Status	Operational status of container.
	Manufacturer Name	Name of manufacturer of container.
	Slot Configuration	Slot configuration of container.
	Container Model Name	Model name of container.
	Container Vendor Type	Vendor type of container.
	Parent Relative Position	Parent Relative Position of container.
	Container Serial Number	Serial number of container.
	Physical Entity Name	Physical entity name of container.
	Description	Description of container.
	Component Type	Type of container component.
	Index	Index of container.
	Field Replaceable Unit	FRU of container.
Fan	Fan Model Name	Name of model of fan.
	Fan Vendor Type	Vendor type of fan.
	Parent Relative Position	Parent Relative Position of fan.
	Fan Serial Number	Serial number of fan.
	Description	Description of fan.
	Physical Entity Name	Physical entity name of fan.
	Component Type	Component type of fan.
	Index	Index of fan.
	Field Replaceable Unit	FRU of fan.
	Alias Name	Alias name of fan.
	Operational Status	Operational status of fan.
	Manufacturer Name	Name of manufacturer of fan.
	Slot Configuration	Slot configuration of fan.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Flash	Module Index	Module index of flash.
Flash Device	Removable	Indicates whether the flash device removable.
	Jumper	Jumper of the flash device.
	Controller	Flash device controller.
	Chip Count	Flash device chip count.
	Size (MB)	Total flash device size in MB.
	Partition Count	Partition count of flash device.
	Maximum Partitions	Maximum partitions in flash device.
	Minimum Partition Size (MB)	Minimum partition size of flash device.
	Name	Name of the flash device.
	Index	Index of flash device.
	Description	Description of flash device.
Flash File	Index	Flash file index.
	Status	Flash file status.
	Checksum	Checksum of flash file.
	Size (MB)	Size of flash file.
	Name	Name of flash file.
Flash Partition	Algorithm	Algorithm of the flash partition
	Filename Length	Flash filename length.
	Erase Needed	Whether an erase is needed.
	Upgrade Method	Method of upgrade of flash partition.
	Status	Status of flash partition.
	Free (MB)	Free space in MB.
	Size (MB)	Flash partition size in MB.
	Name	Name of flash partition.
	Index	Flash partition index.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
IP Address	IP Address	IP Address of the device.
	Index	IP Address index.
	Address State	IP Address state.
	Address Type	Type of IP Address.
	Protocol of Address	Protocol of IP Address.
	Max Re-assemble Size	Maximum re-assemble size.
	Broadcast Address	Broadcast address.
	Network Mask	Network mask of IP Address.
Image	ROM Sys Version	ROM system software version.
	ROM Version	Version of ROM.
	System Boot Variable	System Boot Variable
	System Image File	System image file.
	Minimum Boot Flash (MB)	Minimum Boot Flash in MB.
	Minimum NVRAM (MB)	Minimum NVRAM in MB.
	Minimum DRAM (MB)	Minimum DRAM in MB.
	Media	Media of image.
	Feature	Image feature
	Module	Image module.
	Image	Software image present on the device.
	Build Time	Build time of image.
	Family	Image family.
	System Description	Image system description.
	Version	Version of the software image on the device.
	Description	Description of image.
	Processor Index	Processor index of image.
Interface	MTU	Maximum transmission unit. Maximum packet size, in bytes, that this interface can handle.
	Alias	Interface alias.
	Last Changed	Time of last change.
	Operational Status	Operational status of interface.
	Admin Status	Administrative status of interface.
	Speed (Mbps)	Speed of interface in Mbps.
	Type	Type of interface.
	Description	Description of interface.
	Name	Name of interface
	Physical Address	Physical address of interface.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Interface	Index	Index of interface.
	Identifier	Identifier of interface.
Memory	Processor Index	Processor index.
	Total Memory (MB)	Total memory in MB.
Memory Pool	Lowest Free Block (MB)	Lowest free block of memory in MB.
	Largest Free Block (MB)	Largest free block of memory in MB.
	Free (MB)	Free memory in MB
	Used (MB)	Used memory in MB.
	Validity	Validity of memory pool.
	Alternate Pool	Alternate memory pool.
	Name	Name of the memory pool.
	Type	Memory pool type.
Module	Parent Relative Position	Parent Relative Position of module.
	Field Replaceable Unit	FRU of module.
	Alias Name	Alias name of module.
	Reset Reason	Module reset reason.
	Admin Status	Administrative status of module
	Additional Status	Additional status of module
	Module IP Address	IP Address of module
	Hardware Encryption	Hardware encryption of module
	Slot Number	Slot number of module
	Inline Power Capable	Inline power capability of module
	Parent Type	Module parent type.
	Multiservice	Is this a multiservice module
	Parent Index	Parent index of module
	Number of Slots	Number of slots in module
	FW Version	Firmware version of module
	SW Version	Software version of module
	HW Version	Module hardware version.
	Operational Status	Operational status of module
	Manufacturer Name	Name of manufacturer of module
	Physical Entity Name	Physical entity name of module
	Slot Configuration	Slot configuration of module
	Model Name	Name of module.
	Vendor Type	Type of vendor for the module.
	Serial Number	Serial number of module.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Module	Description	Description of module
	Component Type	Component type of module
	Index	Index of module
Port	Manufacturer Name	Port manufacturer name.
	Slot Configuration	Slot configuration of port.
	Port Model Name	Model name of port.
	Port Vendor Type	Port vendor type.
	Port Serial Number	Serial number of port.
	Parent Relative Position	Parent Relative Position of port.
	Description	Description of port.
	Component Type	Port component type.
	Physical Entity Name	Physical Entity Name of port.
	Index	Port index.
	Field Replaceable Unit	FRU of port.
	Alias Name	Alias name of port.
	Status	Status of port
	Operational Status	Operational Status of port
Port Interface	Number	Port interface number.
Power Supply	Parent Relative Position	Parent Relative Position of power supply.
	Physical Entity Name	Physical Entity Name of power supply.
	Admin Status	Administrative status of power supply.
	Operational Status	Operational status of power supply.
	Manufacturer Name	Manufacturer Name of power supply.
	Field Replaceable Unit	FRU of power supply.
	Slot Configuration	Slot configuration of power supply.
	Alias Name	Alias name of power supply.
	Power Supply Model Name	Model name of power supply.
	Power Supply Vendor Type	Vendor type of power supply.
	Power Supply Serial Number	Serial number of power supply.
	Description	Description of power supply.
	Component Type	Component type of power supply.
	Index	Index of power supply.
Processor	Field Replaceable Unit	Processor FRU.
	Alias Name	Alias name of processor.
	Slot Number	Slot number of processor.
	Parent Type	Parent type of processor.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Processor	Parent Index	Parent index of processor.
	Reboot Config Register Value	Reboot configuration register value.
	Config Register Value	Configuration register value
	Physical Entity Name	Name of physical entity.
	NVRAM Used (KB)	Size of the processor NVRAM that has been utilized, in KB.
	NVRAM Size (KB)	Size of the processor NVRAM in KB.
	RAM Size (MB)	Size of processor RAM in MB.
	Operational Status	Operational status of processor.
	Manufacturer Name	Manufacturer name of processor.
	Slot Configuration	Slot configuration of processor.
	Model Name	Name of the processor model.
	Reset Reason	Processor reset reason.
	Vendor Type	Processor vendor type.
	Admin Status	Administrative status of processor.
	Serial Number	Serial number of processor.
	Additional Status	Additional status of processor.
	Description	Description of processor.
	Module IP Address	Module IP Address of processor.
	Component Type	Component type of processor.
	Hardware Encryption	Hardware encryption.
	Index	Index of processor.
	Inline Power Capable	Inline power capability of processor.
	Multiservice	Multiservice.
	Number of Slots	Number of slots in processor.
	FW Version	Firmware version of processor.
	SW Version	Software version of processor.
	HW Version	Hardware version of processor.
	Parent Relative Position	Parent Relative Position of processor.
Sensor	Parent Relative Position	Parent Relative Position of sensor.
	Physical Entity Name	Name of physical entity of sensor.
	Operational Status	Operational status of sensor
	Manufacturer Name	Manufacturer name of sensor
	Field Replaceable Unit	FRU of sensor
	Alias Name	Alias name of sensor
	Slot Configuration	Slot configuration of sensor

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Sensor	Sensor Model Name	Model name of sensor
	Sensor Vendor Type	Vendor type of sensor
	Sensor Serial Number	Serial number of sensor
	Description	Description of sensor
	Component Type	Component type of sensor
	Index	Index of sensor
Slot	Serial Number	Serial number of slot.
	Description	Description of slot.
	Component Type	Component type of slot.
	Index	Index of slot.
	Parent Relative Position	Parent Relative Position of slot.
	Physical Entity Name	Physical Entity Name of slot.
	Operational Status	Operational Status of slot.
	Manufacturer Name	Name of manufacturer of slot.
	Field Replaceable Unit	FRU of slot.
	Slot Configuration	Configuration of slot.
	Alias Name	Alias name of slot.
	Model Name	Model name of slot.
	Vendor Type	Vendor type of slot.
Stack	Field Replaceable Unit	FRU of stack.
	Operational Status	Operational status of stack.
	Alias Name	Alias name of stack
	Manufacturer Name	Manufacturer name of stack
	Slot Configuration	Slot configuration of stack
	Stack Model Name	Model name of stack
	Stack Vendor Type	Vendor type of stack
	Stack Serial Number	Serial number of stack
	Description	Description of stack
	Parent Relative Position	Parent Relative Position of stack
	Component Type	Stack component type.
	Index	Index of stack.
	Physical Entity Name	Physical Entity Name of stack.
Sys Application	Index	Index of system application
	Software Serial Number	Software serial number of system application.
	Software Version	Software version of system application
	Software Product Name	Name of software product.

Table 6-3 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Sys Application	Software Manufacturer	Software manufacturer of system application
System	SysUpTime	System Up Time.
	Host Name	Host name of the system
	Management Type	Management type of system.
	Modular	Modularity of system.
	OSI Layer Services	OSI layer services of system.
	System Name	System name.
	System Object ID	System Object ID of the device.
	Location	System location.
	Contact	System contact.
	Domain Name	Domain name of the system.
	Description	Description of the system.

Changing the Schedule for System Inventory Collection or Polling

At the time of RME installation, system jobs are created for both Inventory collection and polling, with their own default schedules. A periodic inventory collection job collects inventory data from all managed devices and updates your inventory database.

Similarly, the periodic polling polls devices and updates the inventory database. You can change the schedule of these default, periodic system jobs.

For inventory collection or polling to work, your devices must have accurate read community strings entered. (For the detailed procedure, see the section Adding and Troubleshooting Devices Using Device Management.) The changes detected by inventory collection or polling, are reflected in all associated inventory reports.

Note that the inventory poller allows you to collect inventory less often. The poller detects most changes in managed devices, with much less impact on your network. If the poller detects changes, it initiates inventory collection. To collect inventory or poll devices as a one-time event or for selected devices only, create user-defined inventory collection or polling jobs (see Creating and Editing an Inventory Collection or Polling Job).

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform these tasks.

Step 1 Select **Resource Manager Essentials > Admin > Inventory > System Job Schedule**.

The System Job Schedule dialog box displays the current collection or polling schedule. It is divided into two panes:

- Job Type: Inventory Collection
- Job Type: Inventory Polling

The fields in these panes are identical. You can enter date for either collection and polling, or both.

Step 2 Click **Apply** in the respective panes for the changes to take effect.

Step 3 Set the new Inventory Collection or Inventory Polling schedule in the respective panes, as follows:

Field	Description
Scheduling	
Run Type	Select the run type or frequency for inventory collection or polling—Daily, Weekly, or Monthly. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	Select the date for the collection or polling to begin, using the date picker.
at	Enter the time for the collection or polling to begin, in the hh:mm:ss format.
Job Info	
Job Description	Has a default Job Description: For Job Type, Inventory Collection, the description is, System Inventory Collection Job. For Job Type, Inventory Polling, the description is, System Inventory Polling Job.
E-mail	Enter e-mail addresses to which the job sends messages when the collection or polling job has run. You can enter multiple e-mail addresses, separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender’s address.

Inventory data does not change frequently, so infrequent collection is better. However, if you are installing much new equipment, you may need more frequent collection.

Infrequent collection reduces the load on your network and managed devices. Collection is also best done at night or when network activity is low.

Also, make sure your collections do not overlap, by checking their duration using the Inventory Job Browser (see Using the Inventory Job Browser), and scheduling accordingly.

Step 4 Click **Apply**.

The new schedule is saved.

Cisco.com Fetch Interval

You can use Cisco.com Fetch Interval to determine the frequency at which the information can be retrieved from Cisco.com for generating:

- PSIRT Summary Report (see Generating a PSIRT Summary Report for more information)

- End of Sale/End of Life Report (see Generating End of Sale/End of Life Report for more information)

To set the Cisco.com Fetch interval:

Step 1 Select **Resource Manager Essentials > Admin > Inventory > Cisco.com Fetch Interval**

The Cisco.com Fetch Interval dialog box appears.

Step 2 Select a frequency at which you require the PSIRT information to be retrieved from Cisco.com.

The duration can be:

- 1 hour
- 3 hours
- 24 hours - this is default value
- 7 days
- 30 days

Step 3 Select a frequency at which you require the End of Sale/End of Life information to be retrieved from Cisco.com.

The duration can be:

- 1 hour
- 3 hours
- 24 hours
- 7 days - this is default value
- 30 days

Step 4 Either:

- Click **Apply** to apply the changes.

Or

- Click **Cancel** to revert your selections to the last saved value.

Generating Inventory Reports

You can use the Inventory reports option to examine your default and custom reports.

Using the Report Generator of RME, you can generate the following Inventory reports and graphs:

- 24-Hour Inventory Change Report (see Generating a 24 Hour Inventory Change Report).
- Chassis Slot Details (see Generating Chassis Slot Details).
- Chassis Slot Summary (see Generating a Chassis Slot Summary).
- Detailed Device Report (see Generating a Detailed Device Report).
- Hardware Report (see Generating a Hardware Report).
- Software Report (see Generating a Software Report).
- PSIRT Summary Report (see Generating a PSIRT Summary Report)

- EoSale/EoL Report (see Generating End of Sale/End of Life Report)
- MultiService Port Details (see Generating MultiService Port Details).
- Hardware Summary Graph (see Generating a Hardware Summary Graph).
- Software Version Graph (see Generating a Software Version Graph).
- Chassis Summary Graph (see Generating a Chassis Summary Graph).

You can run Inventory reports and graphs on multiple clients concurrently. While the reports can be run immediately or scheduled to run at a later date, the graphs can only be run immediately.

Successfully generated reports are stored in the Archives. You can access the reports archives by selecting **Resource Manager Essentials >Reports > Report Archives** (see the topic Viewing Archived Reports in the section Generating Reports).

In the Reports Archive/Report jobs, you cannot see the Immediate Run Type reports.

An Immediate job displays the first 10,000 lines of a report. For the full report, schedule a job.

If you have selected the Run Type as Immediate, the report appears in a separate browser window.

If you have selected an option other than Immediate in the Run Type field, then a message is displayed,

```
Job ID created successfully.
Go to Reports > Report Jobs to view the job status.
```

Here, Job ID is a unique Job number.

You can cross-launch to Device Centre by clicking the device names hyperlink, in the generated reports. For details see Using Device Center for Inventory Tasks.

To purge archived reports and report jobs, see the topic Purging Reports Jobs and Archived Reports in the section Generating Reports.

To use the Report Generator:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, and select **Inventory**.

Step 3 Go to the second drop-down list box, select the required report, for example, 24-Hour Inventory Change Report.

Step 4 Select the required devices using the Device Selector. (See the topic, Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management, for more details.)

Step 5 Enter the information required to generate the required report:

Field	Description
Scheduling	
Run Type	Specifies the type of schedule for the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. If you select Immediate, all other options are disabled.
Run Type (continued)	If you select any of the other frequencies, then you can specify the start date and time and also provide this information: • Job Description—Enter the description of the job. A mandatory field. Enter up to 256 characters (alphanumeric). • E-mail ID—Enter e-mail addresses to which the job sends messages for notification that has to be sent after the report is run. An optional field. You can enter multiple e-mail addresses, separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address. • Report Publish Path—This is the location on the RME server where an HTML version of the report will be saved. An optional field.
Date	Click on the calendar icon and select the date. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field. Select the hours and minutes from the drop-down lists.
Job Info	
Job Description	Enter a description for the report that you are scheduling. The Job Description field is enabled only if you have selected an option other than Immediate in the Run Type field. This is a mandatory field. Accepts alphanumeric values. The field is restricted to 256 characters.

Field	Description
E-mail	Enter a valid e-mail ID of the users who should be notified when the report job has run. You can enter multiple e-mail addresses, separated by commas. Configure the SMTP server to send e-mails in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field.
Report Publish Path	Enter a location on the RME server (file path with a valid file name), where an HTML version of the report will be saved. The file name that you specify may be a non-existent file in an existing folder or a new file in a new folder. Causer should have write permissions to the given folder. The following message appears if an invalid file name is specified or the casuser is unable to create file in given folder: `Failed to create` *filename*`. Check directory permission for casuser and/or provide a valid file name.` Alternatively, to select a location, click **Browse**. The Server Side File Browser dialog box appears. In the Server Side File Browser dialog box: **1.** Select the directory content. **2.** Select the drive. The location appears in the File field. **3.** Click **OK**. The specified location appears in the Report Publish Path in the RME reports dialog box. This field does not appear while scheduling PSIRT Summary Report and EoSale/EoL Report.
Report Display Format	
Attributes in a Single Table	Select this option to view all the attributes that you chose while creating the custom report, in a single table. This option is only available for a Inventory custom report. This field does not appear while scheduling PSIRT Summary Report and EoSale/EoL Report.
Attributes in Multiple Tables	Select this option to view the report, grouped by the attributes that you chose while creating the custom report. This option is only available for a Inventory custom report. This field does not appear while scheduling PSIRT Summary Report and EoSale/EoL Report.

Field	Description
Cisco.com Profile	
Cisco.com User Name	Enter your Cisco.com username.
Cisco.com Password	Enter your Cisco.com password.
Proxy User Name	Enter your Proxy username. You are prompted to enter a Proxy username only if a Proxy Server hostname/IP and port are configured in Common Services > Security > Cisco.com Connection Management Proxy Server Setup
Proxy Password	Enter your Proxy password. You are prompted to enter a Proxy password only if a Proxy Server hostname/IP and port are configured in Common Services > Security > Cisco.com Connection Management Proxy Server Setup

Step 6 Click **Finish**.

The specified report appears in a separate browser window.

Click **Reset All** to reset your selections for *all* groups. This resets all previous values to blanks.

In the generated report you can perform the following tasks:

- Use the Export Current Report icon to export the generated report to a PDF or a comma separated values (CSV) format.
- Use the Printer Friendly Format icon to generate a printer-friendly format for the displayed report.
- Use the Export Device List to Device Selector icon to export the list of devices for which the report has been generated, to the Device Selector. You can use this list to perform specific tasks or perform an action based on the report.
- Sort the contents of any table, by clicking on the table heads.

Generating a 24 Hour Inventory Change Report

The 24-Hour Inventory Change Report shows the details of all inventory changes made during the last 24 hours. This report displays the changes in the values of the attributes of each device that has undergone a change in the last 24 hours, with the time stamp.

To view changes made beyond the last 24 hours, use the Change Audit application, which displays all application changes.

To refer to the 24-Hour Inventory Change Report regularly, you should schedule inventory collection to run every 24 hours. For details on scheduling inventory collection see Creating and Editing an Inventory Collection or Polling Job.

To generate the report, see Generating Inventory Reports.

The 24-Hour Inventory Change Report displays:

- The following device details:
  - Total number of submitted device(s)
  - No. of device(s) with data

  - Device(s) with change
- Information about the following:
  - Attribute
  - Type of Change
  - Time Change Detected
  - Previous Value
  - Current Value

Generating a Hardware Report

You can generate a report to display detailed hardware information for your selected devices. The Hardware Report includes user-specified information for each device. This user-specified information will be displayed only when it is available.

To generate the report, see Generating Inventory Reports.

This report displays:

- The following information about hardware characteristics:
  - Total number of devices
  - Devices with inventory data
  - Devices without inventory data
- Details of hardware information including system, processor, chassis information, based on the Cisco MetaData Framework (MDF) categories of devices, with a separate table for each device category.

  Each table displays the hardware information obtained by polling the class-specific MIB objects on the devices.

The flash size that appears in the Hardware Report is the total of the flash sizes of all the flash devices on that particular device.

For example, if you have a Catalyst 4503 device that contains flash devices such as Boot Flash (61000000 bytes), Slot0 Compact Flash (128000000 bytes), and Cat4000 Private Flash (500000 bytes), the Hardware Report for this Catalyst device will display the total of all the flash devices. That is, the sum of the Boot Flash, Slot0 Compact Flash, and Cat4000 Private Flash (189500000 bytes).

You can also use Custom Reports (see Using Inventory Custom Report Templates) to generate more specific information, such as RAM size, flash size, port count, hardware version, or card type.

From within the report, you can access any table in the report using the Go to Device category drop-down list. This list displays all the device categories in the generated report.

For more information about a device in the report, click on the device name or IP address. You will be directed to Device Center. (For details about Device Center, see the CiscoWorks Common Services Online Help or User Guide).

Generating a Software Report

You can display software information including system information, image information and processor details for selected devices. User-specified information is also displayed in this report, when it is available.

The report contains a different table for each device category based on the Cisco MetaData Framework (MDF) categorization. Each table summarizes the software information obtained by polling the class-specific MIB objects on the devices.

To generate the report, see Generating Inventory Reports.

From within the report, you can access any table in the report using the Go to Device category drop-down list. This list displays all the device categories in the generated report.

For more information about a device in the report, click on the device name or IP address. You will be directed to Device Center. (For details about Device Center, see the CiscoWorks Common Services Online Help or User Guide.)

Generating a Detailed Device Report

You can display complete inventory information for selected devices.

The Detailed Device report displays detailed hardware, software characteristics, characteristics including System, Port Interface, Bridge, Memory Pool, Flash Devices, Image, and physical containment information, such as Stack, Chassis, Module, Processor information, for one or more selected devices.

Device information is obtained by polling the class-specific MIB objects on the devices that you select. You can view interface administrative status and slot details for some device classes.

The information shown in this report is based on:

- Physical inventory information (all physical components on the device containment like Stack, Back Plane, Chassis, module, Power Supplies, Fan, Processor).
- Flash and Memory information.
- Logical Inventory Information (logical aspects such as Interfaces, Bridge Interface, Application Information).
- System Information (RFC 1213 system information).
- Asset Information (information on Asset Tracking).

The Detailed Device Report also displays the Unique Device Identifier (UDI) for all the components of a device. UDI is unique to each component of a device. It is a combination of Product Identifier (PID), Version Identifier (VID) and Serial Number (SN).

Total Memory in the Memory Information table of the Detailed device report is computed as follows:

- For routers that query for processorRam value from Old-Cisco-Chassis-Mib:

  Total Memory = Processor memory + I/O memory (buffer memory)
- For all other devices, whenever available from the MIB:

  Total Memory = Processor memory.

Note Some data is not displayed, if you have not yet run inventory collection.

To generate the report, see Generating Inventory Reports.

Click on a device name to see details for that device.

From within the report, you can access any table in the report using the Go to Device category drop-down list. This list displays all the device categories in the generated report.

Generating a Chassis Slot Summary

For each device category that supports capacity planning, the Chassis Slot Summary shows the total number of devices and the number of devices with free slots.

You can click on a link to display Chassis Slot Details for those devices, for example, all devices with free slots.

You can display the number of available slots for the following device classes:

- Cisco Catalyst Switch
- Cisco Router
- Cisco Aironet
- Cisco LS1010 Switch
- Cisco Catalyst L2L3 Switch

The report also displays a summary of the devices submitted for the report, the number of devices that are without data, and the devices that do not support capacity planning.

To generate the report, see Generating Inventory Reports.

Generating Chassis Slot Details

The Chassis Slot Details report is for those devices that support Chassis capacity. The report displays the number of free slots or the available capacity for the selected devices.

The devices that support capacity planning include Catalyst Switch, L2L3 Switch, and Router.

To generate the report, see Generating Inventory Reports.

This report displays the device name, the total slots, the available slots, location of the device, and userfield information for each device, based on the Cisco MetaData Framework (MDF) categorization.

The report also displays a summary of the devices submitted for the report, the number of devices that are without data and the devices that do not support capacity planning.

Click on a device name to go to Device Center. (For details about Device Center, see the CiscoWorks Common Services Online Help or User Guide).

Generating MultiService Port Details

You can display information about multiservice ports on selected switches. Multiservice ports are specially designed to supply inline power while supporting voice traffic.

This report displays devices and the number of free slots, and multi-service ports available. The report displays information such as device name, domain name, total slots, available slots, location, power supply, multi-service port modules, module port count, powered port count, and user-defined fields.

This report is applicable for modular devices such as Catalyst 4000, Catalyst 6000.

If you want your system to support voice traffic, use this report to determine:

- Whether your switch has empty slots into which you can install multiservice modules (Available Slots).
- Whether you have to upgrade your power supply wattage to support the multiservice modules installed in your switch (Power Supply and Multiservice Modules).

- Whether any multiservice modules require submodule installation (Module Port Count vs. Powered Port Count).
- How many ports are ready to provide in-line power (Powered Port Count).

To generate the report, see Generating Inventory Reports.

Click on a device name to go to Device Center. (For details about Device Center, see the CiscoWorks Common Services Online Help or User Guide).

The information in the MultiService Port Details report is updated during the regular inventory collection. You can manually update:

- User fields with Change Device Credentials.
- The Location field with the CLI as described in the device's configuration guide.

Generating a Hardware Summary Graph

You can display a pie graph showing the distribution of all managed Cisco devices in the inventory. The graph plots the percentage count of devices, based on the Cisco MetaData Framework (MDF) categorization of devices (Level 2 categorization).

Each section represents the device category, the device count and percentage of the total devices.

To generate the report, see Generating Inventory Reports. After Step 4, click **Finish**. The Hardware Summary Graph appears. You cannot schedule the generation of this graph.

This graph displays:

- The device category and the percentage of distribution in the network.
- The Count. Click **Count** to view the Hardware Report for that device category (see Generating a Hardware Report.)
- The hardware summary, which identifies each section of the graph.

Generating a Software Version Graph

You can generate a pie graph to show the distribution of major and minor Cisco software versions running on the devices in a network. The graph plots the percentage count of selected devices from Inventory, based on the Cisco MetaData Framework (MDF) categorization of devices.

To generate the report, see Generating Inventory Reports.

After Step 4, click **Finish**. The Software Version Graph appears. You cannot schedule the generation of this graph.

This graph displays:

- The Software Version and the percentage.
- The Count. Click **Count** to view the Software Report for that device category (see Generating a Software Report.)
- The software version summary, which identified each section of the graph.

Generating a Chassis Summary Graph

You can generate a pie graph to show the distribution of all Cisco devices in the inventory. The graph plots the percentage count of devices, based on the Cisco MetaData Framework (MDF) categorization of devices (Level 2 and Level 3 categorization).

You can click on any to view a hardware report. Generating a Hardware Report.

To generate the report, see Generating Inventory Reports. After Step 4, click **Finish**. The Chassis Summary Graph appears. You cannot schedule the generation of this graph.

The Chassis Summary Graph displays information about the devices categories, their percentage and the count. Click **Count** to view the Hardware Report for that device category (see Generating a Hardware Report.)

Generating a PSIRT Summary Report

Cisco's Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability-related information, related to Cisco products and networks.

For evey security vulnerability, a PSIRT document is created with a PSIRT Document ID. This document consists of the definition of the vulnerabilities, the IOS image version that is affect by the PSIRT as well as the device that is impacted.

RME provides for the fetching and collection of these PSIRT information from Cisco.com at regular intervals.

See Cisco.com Fetch Interval for more information on setting or changing the frequency of retrieval of PSIRT information from Cisco.com.

You can generate a PSIRT Summary Report based on the PSIRT information retrived from Cisco.com at regular intervals. This report helps you in ascertaining the security vulnerabilities that affect the devices in your network.

It provides a summary of the possible security alerts based on the selected devices. It also recommends upgrade to the IOS image version which has the fix for the security vulnerability.

To generate the report, see Generating Inventory Reports.

The generated PSIRT Report shows:

- Count of the Total number of Devices selected for report generation.
- Count of devices with vulnerability
- Last Cisco.com Fetch Date
- Two tables categorized based on:
  - PSIRT ID
  - Device

The **By PSIRT** table displays the following fields:

- PSIRT Document ID
- Announcement Date
- Description
- Severity

- IOS Version(s) Impacted
- Image File Name(s)
- Number of devices affected
- Fixed in IOS Version(s)

Click on a specific field Id to sort the information based on a this field.

The **By Device** table displays the following fields:

- Device Name / IP Address
- Device Model
- PSIRT Document ID
- IOS Version
- Location

Click on any field id to sort the information based on a selected field.

For more information on the fields in the PSIRT Summary report tables, see Fields in the PSIRT Summary Report Tables.

You can also click on:

- Any of the PSIRT Document id link to get more information about the devices affected by that PSIRT ID. On clicking the PSIRT Document ID an external web page is opened with more details of that particular PSIRT.

Or

- The Number of Affected Devices link to get more information about the devices affected by a corresponding PSIRT ID. When you click the Number of Affected Devices link, the By Devices table is displayed. The devices affected by the corresponding PSIRT is listed at the top of the table.

Note The PSIRT Summary report displays PSIRTs only for Cisco IOS device categories.

Fields in the PSIRT Summary Report Tables

Table 6-4 provides description for the fields in the By PSIRT table.

Table 6-4 Fields in the By PSIRT Table

Field	Description
PSIRT Document Id	Document ID of the PSIRT announcement. Click on the PSIRT Document ID for more information on that PSIRT.
Announced Date	Date on which the PSIRT announcement was released in Cisco.com.
Description	Brief description of the security vulnerability.
Severity	Severity classification for the PSIRT. It could be: • High • Medium • Low
IOS Version(s) Impacted	IOS software version that is impacted by the PSIRT.

Field	Description
Image File Name(s)	Name of the image file.
Number of devices affected	Count of the number of devices affected by the PSIRT.
Fixed in IOS Versions(s)	IOS software version that has the fix to the security vulnerability. You can upgrade to this fixed IOS version to overcome the security vulnerability.

Table 6-5 provides description for the fields in the By Device table.

Table 6-5 Fields in the By Device Table

Field	Description
Device Name	Name or IP address of the device.
Device Model	Model of the device.
PSIRT Document Id	Document ID of the PSIRT announcement. Click on the PSIRT Document ID for more information on that PSIRT.
IOS Version	IOS software version that is impacted by the PSIRT.
Location	Physical location of the device in the network.

Generating End of Sale/End of Life Report

The End of Sale information for a device refers to announcement made in Cisco.com regarding the ending of sales of a device or hardware.

The End of Life information refers to announcement made in Cisco.com of the ceasing of production of a device or hardware.

RME provides for the fetching and collection of these End of Sale/End of Life information from Cisco.com at regular intervals.

See Cisco.com Fetch Interval for more information on setting or changing the frequency of retrieval of End of Sale/End of Life information from Cisco.com.

You can generate a End of Sale/End of Life Summary Report based on the end of sale/end of life information retrieved from Cisco.com at regular intervals. This report helps you in ascertaining the end of sale/ end of life information for devices and modules in your network. It provides a summary of the end of sale or end of life alerts based on the selected devices.

To generate the report, see Generating Inventory Reports.

The generated End of Sale/End of Life Report shows:

- Count of the Total number of Devices selected for report generation.
- Count of devices with End of Sale/End of Life announcements.
- Count of modules with End of Sale/End of Life announcements.
- Last Cisco.com Fetch Date
- Three tables categorized based on:
  - End of Sale/End of Life announcements
  - Modules with End of Sale/End of Life announcements

  - Devices with End of Sale/End of Life announcements

The **End of Sale/End of Life Announcements for Devices** table displays the following fields:

- Bulletin Number
- Device Model
- Number of Devices
- EOS Date
- EOL Date

Click on a specific field ID to sort the information based on this field.

The **End of Sale/End of Life Announcements per Module** table displays the following fields:

- Bulletin Number
- Module Type
- Number of Modules
- EOS Date
- EOL Date

Click on a specific field ID to sort the information based on this field.

The **Devices that have End of Sales / Support Announcements** table displays the following fields:

- Device Name
- Device Model
- Module Type
- Location
- Bulletin Number

Click on a specific field ID to sort the information based on this field.

For more information on the fields in the End of Sale/End of Life report tables see Fields in the End of Sale/End of Life Report Tables.

If you:

- Click on the Number of Devices link from the End of Sales/End of Life Announcements for devices table, the devices that have End of Sales/End of Life support announcements table is displayed.

  The records are arranged according to the Bulletin Number that correspond to the Number of Devices link clicked in the End of Sales/End of Life Announcements for devices table.
- Click on the Number of Modules link from the End of Sales/End of Life Announcements for modules table, the Devices that have End of Sales/End of Life support announcements table is displayed.

  The records are arranged according to the Bulletin Number that corresponds to the Number of Modules link clicked in the End of Sales/End of Life Announcements per module table.

Fields in the End of Sale/End of Life Report Tables

Table 6-6 provides descriptions for the fields in the End of Sales / End of Life Announcements for Devices table.

Table 6-6 Fields in the End of Sales / End of Life Announcements for Devices Table

Field	Description
Bulletin Number	Bulletin number of End of Sale / End of Life Announcement for a device in Cisco.com. Click on the bulletin number link for more information of End of Sale / End of Life Announcement for that device in Cisco.com. There maybe multiple announcements for a device.
Device Model	Model of the device. For instance, the device model can be Cisco Catalyst 4507R Switch.
Number of devices	Count of the number of affected devices.
EOS Date	Last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.
EOL Date	Date the document that announces the end of sale and end of life of a product is distributed to the general public.

Table 6-7 provides descriptions for the fields in the End of Sales / End of Life Announcements Per Module table.

Table 6-7 Fields in the End of Sales / End of Life Announcements Per Module table

Field	Description
Bulletin Number	Bulletin number of End of Sale / End of Life Announcement for a module in Cisco.com. Click on the bulletin number link for more information of End of Sale / End of Life Announcement for that module in Cisco.com. There maybe multiple announcements for a module.
Module Type	Module type information consisting of the End of Sale product part number.
Number of Modules	Count of the number of affected modules.
EOS Date	Last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.
EOL Date	Date the document that announces the end of sale and end of life of a product is distributed to the general public.

Table 6-8 provides descriptions for the fields in the Devices that have End of Sales / Support Announcements table.

Table 6-8 Fields in the Devices That Have End of Sales / Support Announcements Table

Field	Description
Device Name	Name or IP address of the device. Click on the device name for more information about the device.
Device Model	Model of the device. For instance, the device model can be Cisco Catalyst 4507R Switch.
Module Type	Module type information consisting of the End of Sale product part number.

Field	Description
Location	Physical location of the devices on the network.
Bulletin Number	Bulletin number of End of Sale / End of Life Announcement for a device or module in Cisco.com. Click on the bulletin number link for more information of End of Sale / End of Life Announcement for that device or module in Cisco.com. There maybe multiple announcements for a device or module.

Using Inventory Custom Report Templates

The Custom Templates option lets you create new report templates customized according to your requirements. You can also edit, or delete existing custom templates.

When you select **Resource Manager Essentials > Reports > Custom Report Templates**, a list of all custom templates is displayed in the dialog box on the Custom Templates page.

The columns in the Custom Templates dialog box are:

Column	Description
Template Name	Name of the template. If you click on this hyperlink, the details of the template are displayed in a pop-up window.
Report Type	Syslog report, or inventory report.
Owner	User who created the template.
Last Modified Time	Date (yyyy-mm-dd) and the time (hh:mm:ss).

Using the custom templates dialog box, you can do the following tasks:

Task	Button
Create a custom template (see Creating a Custom Report Template).	Create
Modifying a custom template (see Modifying a Custom Template).	Edit
Delete a custom template (see Deleting a Custom Template).	Delete

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform these tasks.

Creating a Custom Report Template

You can create a custom report template for Inventory.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To create a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The Custom Templates dialog box appears.

Step 2 Click **Create**.

The Application Selection dialog box appears.

Step 3 Select Inventory.

Step 4 Click **Next**.

The Template Properties dialog box appears.

Step 5 Enter a unique name for the custom report template, in the Report Name field.

This is a mandatory field. You can use the character set for the template names including A to Z, a to z, 0 to 9, -, _, .,), (, / and blank spaces. The report name should not exceed 60 characters.

Step 6 Specify whether you want the template to available for Public access, or Private access.

Templates that you specify as Public can be seen by other users who are authorized to view this page. Such users can also generate reports on public Templates.

Private templates can be seen by the system administrator and the owner (creator) of the templates. However, only the owner (creator) can generate reports on these Private templates.

Step 7 Click **Next**.

The Custom Template Rules dialog box appears.

Step 8 Use the Custom Template Rules dialog box, to:

- Add a rule (see Adding a Rule).
- Modify a rule (see Modifying a Rule).
- Delete a rule (see Deleting a Rule).

The Custom Template Rules dialog box has these buttons:

- Add—Adds a rule to the custom template (see Adding a Rule).
- Save Changes—Saves the changes that you made to a rule. This button is available only if you select a rule in the Rule List. It is used to save the changes that you made to an existing Rule. To cancel your changes, click the Discard Changes button (also see Modifying a Rule).
- Delete—Deletes a rule (see Deleting a Rule). You can select one or more rules for deletion. This button is available only if you select a rule the Rule List.
- Discard Changes—Cancels the changes that you made to a rule. This button is available only if you select a rule the Rule List. Click this button if you do not want to save the changes that you have made to an existing rule.

Step 9 Click **Next**.

The Custom Template Summary window appears, with the summary information about the rules that you have created.

A sample summary is as follows:

```
Report Name:  FlashDeviceModel

Access Type:  Private

Template Rules:  Flash Device:Model Name:equals:All
```

Step 10 Click **Finish**.

A confirmation message appears, that the Report template has been created successfully.

The Custom template that you created appears in the Custom Templates dialog box.

Adding a Rule

To add a rule:

Step 1 In the Custom Template Rules dialog box, select information in the following fields:

Field	Description
Association	Select an association. If you are adding a rule for the first time, this drop-down list does not display any values. After you have added a rule and need to add another rule, this drop-down list has the values AND and OR.
Inventory Group	Select the Inventory Group for which you are creating the rule. For details see Table 6-9Inventory Groups and Attributes.
Attribute	Select an attribute. The attributes that are available in the drop-down list are based on the Inventory group that you selected. For example, if you select flash device as the Inventory group, the Attributes available for selection are: • Flash Device Size (MB) • Model Name For details see Table 6-9.
Operator	Select the operator.
Value	Select the value. For example, ALL. By default ALL will be populated along with editable drop down item. (The editable drop-down item is the blank one. You can enter your value in it.) For specific attributes such as VendorType, MemoryType etc., the drop down is be pre-populated when you select the corresponding attributes. For other remaining attributes ALL and Editable (blank field) will be present in the Value drop-down list. You can either select a value from this drop-down list or enter the value by selecting editable list item.

The following are the Inventory Groups and Attributes:

Table 6-9 Inventory Groups and Attributes

Report Inventory Group	Custom Report Group/Attribute	Description
Asset	CLE Identifier	CLE identifier of the asset
	Orderable Part Number	Orderable part number of the asset.
	User-defined Identifier	User-defined identifier of the asset

Table 6-9 Inventory Groups and Attributes (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Chassis	Chassis Model Name	Name of the model.
	Chassis Serial Number	Serial number of the chassis.
	Chassis Vendor Type	Type of vendor for the chassis.
	Chassis Version	Version number of the chassis.
	Number of Slots	Number of slots in that chassis.
	Port Count	Total port count of the chassis.
Device Type	Category	MDF category of the device.
	Series	MDF series of the device.
	Model	MDF model of the device.
Flash Device	Flash Device Size (MB)	Total flash device size in MB.
	Model Name	Model name of the flash device.
Flash File	Path Name	Location of flash file.
	Size (MB)	Flash file size in MB.
Flash Partition	Erase Needed	Whether an erase is needed.
	Free (KB)	Free space in KB.
	Name	Flash partition name.
	Size (MB)	Flash partition size in MB.
Image	Image Version	Version of the software image on the device.
	ROM Sys Version	ROM system software version.
	ROM Version	Version of ROM.
	Sys Description	Image system description.
Interface	Name	Interface name.
	Type	Interface type.
IP Address	IP Address	IP Address of the device.
	Subnet Mask	Subnet mask.
Memory	Size (MB)	Total RAM size.
Memory Pool	Free (MB)	Free memory in MB
	Name	Name of the memory pool.
	Used (MB)	Used memory in MB.
	Type	Memory pool type.
Module	HW Version	Module hardware version.
	Model Name	Name of the model.
	Port Count	Total ports on that module.
	Serial Number	Serial number of the module.
	Vendor Type	Type of vendor for the module.

Table 6-9 Inventory Groups and Attributes (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Processor	Model Name	Name of the model.
	NV RAM Size (KB)	Size of the processor NVRAM in KB.
	NV RAM Used (KB)	Size of the processor NVRAM that has been utilized, in KB.
	PortCount	Total port count of the processor
	RAM Size (MB)	Size of the processor RAM in MB.
	Serial Number	Serial number of the processor.
	Vendor Type	Type of vendor for the processor.
System	Contact	Contact details for the system.
	Description	Description of the system.
	Domain Name	Domain name of the system.
	Location	System location.
	Name	System name.
	System Object ID	System Object ID of the device.
	SysUpTime	System up time. The datatype of this attribute is timestamp and in the following format: yy:mm:dd:hh Where: • yy — number of years, • mm — number of months, • dd— number of days • hh — number of hours.
	User-defined Serial No.	User-defined serial number.
UDF	For example: • User_defined_field_0 • User_defined_field_1 • User_defined_field_2	All User-defined fields defined in Devices and Credentials Repository (DCR) are displayed here.

Step 2 Click **Add** to save the rule.

The rule that you created, appears in the Rules List section. You can add more than one rule.

To understand how RME evaluates rules, see Understanding Template Rules Evaluation.

Modifying a Rule

To modify a rule:

Step 1 Select the required rule from the Rules List section of the Custom Template Rules dialog box.

The values that you had selected previously for this rule, appear in their respective fields.

Step 2 Change these values as required.

Step 3 Click **Save Changes**.

The rule is modified.

If you do not want to save your changes, click **Discard Changes**.

After you select a rule from the Rules List section, you cannot move to the next dialog box by clicking **Next**. A message appears:

```
You are currently modifying a rule. You are not allowed to proceed to the next step until
you complete the current task. Click Save Changes to save the current changes or Discard
Changes to cancel.
```

Deleting a Rule

To delete a rule:

Step 1 Select the required rule from the Rule List section of the Custom Template Rules dialog box. You can select one or more rules for deletion.

Step 2 Click **Delete**.

A message appears prompting you to confirm the deletion. If you confirm the deletion, the rule is deleted.

Modifying a Custom Template

You can modify a custom report template.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To modify a custom template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The Custom Templates dialog box appears with a list of Custom templates.

Step 2 Select the required custom template from the list, and click **Edit**.

The Template Properties dialog box appears. It is prepopulated with your selected template properties.

Step 3 Click **Next**.

The Custom Templates Rules dialog box appears.

For the description of the columns in the Custom Reports Templates dialog box, see Creating a Custom Report Template.

If required, you can modify the template by:

- Adding a Rule
- Modifying a Rule
- Deleting a Rule

Step 4 Click **Next**.

The Custom Template Summary window appears, with the summary information about the rules that you have created.

Step 5 Click **Finish**.

A confirmation message appears, that the Report template has been created successfully.

The modified custom template appears in the custom templates dialog box.

Deleting a Custom Template

You can delete a custom report template for Inventory.

Only users with System Administrator privileges can delete (but not edit) any Public or Private templates created by any user. This privilege is given to the System Administrator to clean up the system when a owner of a template has ceased to exist within the system.

View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

Note If you delete a template, any job created with the template will fail.

To delete a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The custom templates dialog box appears with a list of custom templates.

Step 2 Select the required custom template. You can select one or more custom templates to delete.

Step 3 Click **Delete**.

A message appears prompting you to confirm the deletion.

If you confirm the deletion, the template is deleted and will not appear in the Inventory custom report template dialog box.

Understanding Template Rules Evaluation

This section helps you understand how the template rules are evaluated by RME:

- Rules are evaluated from 1to n (left to right).
- The rules with AND operators will be evaluated first and then the OR operator will be applied on the AND operator results.

If a template has rules a, b, c and d and the are given as a AND b OR c AND d, this set of will be evaluated as (a AND b) OR (c AND d).

- If you want to just see the data for a set of attributes, you can:
  - Choose the group and attribute without any operator and value.

    or

  - Choose the group and attribute with any operator and value the should be ALL. The association string can be either AND or OR.

    This is only when there is no criteria for any of the rule, and you want to view the data for a set of attributes.

Since bracketization is not supported for rules, you should define the template rules intelligently after understanding the evaluation mechanisms (see Understanding Template Rules Evaluation).

Also, if you want to order the rules, then you need to delete the existing rules and add them again required, or redefine the template, that is, delete and create it anew.

Running a Custom Report

You can run any custom report that you previously created. When you run the report, Inventory uses the criteria you specified when you created the report (see Using Inventory Custom Report Templates) and displays information on the devices that match.

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Select Inventory, from the first drop-down list.

Step 3 Select the required custom report from the second drop-down list. (Custom reports that you created appear in the drop-down list box with a separator).

The Device Selector appears, along with the fields that allow you to enter information in the Scheduling and Job Info fields.

Step 4 Select the required devices using the Device Selector.

See the topic, Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management, for more details.

Step 5 Enter the information required to generate the required custom report, in the Scheduling and Job Info groups.

For the field descriptions, see Generating Inventory Reports

The custom report appears. See Custom Report Output.

Custom Report Output

A custom report will be generated only if at least one device satisfies the criteria specified in the template. If none of the criteria that you have specified are met, an appropriate message appears to inform you of this.

In the generated report, the legend N/A (Not Applicable) is displayed in the report cells in these cases:

- If that attribute is not collected.
- If the criterion is not applicable to that device.
- If that attribute is user-defined, and has not been configured. (For example, User-defined fields, User-defined Serial Number, etc.).

If a template has a rule with ALL as the criteria, it means, that all the values of this attribute appear for the submitted devices.

If a template rule has no operator, then the values will be assumed as they are with ALL.

The Summary section of the custom reports displays the following information:

- Number of devices selected—Number of devices that you have submitted for report generation.
- Number of devices that do not match criteria—Number of devices not meeting the specified template criteria or rules.
- Number of devices that do not have inventory collected data—Number of devices for which inventory is not collected.

  For example, if *n* number of devices were submitted, *x* devices have inventory collected data and *y* have no inventory collected data. *m* number of devices do not satisfy criteria. This means, this number is out of *n,* irrespective of *y*.

  The number of devices that do not satisfy criteria comes out of the number of devices that were submitted for collection, irrespective of the number of devices for which no inventory was collected.

You can sort on the columns of the report by clicking on the column title. These are the icons on this page

..

Icon	Description
Export Device List to Device Selector (Icon)	Use this icon, if you want to export the device list to Device Selector. For more information, see Exporting Device List to Device Selector.
Export (Icon)	Use this icon if you want to export the report output to a PDF or CSV file. For more information see Exporting Custom report output to a file.
Print (Icon)	Use this icon to print the report output.

Exporting Device List to Device Selector

To export device list from the custom report output to device selector:

Step 1 Go to the Inventory Custom report output page and click **Export**.

The Export Device List dialog box appears.

Step 2 Either:

Click **Yes**, if you want to export the device list to device selector.

Or

Click **No**, if you do not want to export the device list to device selector.

On successful export of the devices, the following message is displayed.

```
Device List exported successfully.
```

Exporting Custom report output to a file

To export custom report output to a file:

Step 1 Go to the Inventory Custom report output page and click **Export**.

The Exporting Report dialog box appears.

Step 2 Either:

Check **PDF** option, if you want to export your report to a PDF file format.

Or

Check **CSV** option, if you want to export your report to a CSV file format.

Step 3 Click **OK** if you want to accept the changes

Or

Click **Cancel** if you do not want to save the changes and close the window.

Examples of Custom Template Definitions

This section contains examples of template definition and the expected output.

- Template Definition Example 1
- Template Definition Example 2
- Template Definition Example 3
- Template Definition Example 4
- Template Definition Example 5
- Template Definition Example 6
- Template Definition Example 7
- Template Definition Example 8
- Template Definition Example 9
- Template Definition Example 10
- Template Definition Example 11
- Template Definition Example 12

Note If any of the selected devices do not satisfy the criteria that you have specified, a message appears: `None of the selected devices match the specified criteria.`

Template Definition Example 1

If you create the rule `IPAddress:IPAddress:contains:1`, in the custom report output, you will get all the IP address of devices which contains `1` as part of the IP Address.

Template Definition Example 2

If the you want to see the device chassis, vendor type, port count of module and processor whose chassis vendor type is xyz and module port count > 0 or Processor port count > 0, the template definition is:

```
Chassis:VendofType:equals:xyz

AND:Module:PortCount:>:0

OR:Chassis:VendofType:equals:xyz

AND:Processor:PortCount:>:0
```

In general mathematical notation, if you want to get the result of A AND (B OR C) where A, B and C are the rules, you need to define as A AND B OR A AND C. RME looks at treats this as (A AND B) OR (A AND C).

The default evaluation by RME is that be all rule blocks associated with AND are evaluated first and then in the next step of evaluation OR is applied on the resultant blocks. That is, all rules with the association string AND are clubbed together and evaluated.

Template Definition Example 3

If you want to get details of the IP Addresses of devices which contain 10.36 or whose devices Memory Type is I/O, then the template definition is:

```
TemplateDef: IPAddress:IPAddress:contains:10.36

OR:Memory:Type:equals:I/O
```

The custom report is generated with all the IP Addresses and Memory Types for the devices having IP Address 10.36 or whose memory type is I/O.

Template Definition Example 4

If you want to get details of the image versions devices which contain 1 and want to know their flash size, then the template definition is:

```
Image:Image Version:contains:1

AND:Flash File:Size (MB)
```

The custom report is generated with the Flash File size and the image version of all the devices whose image version contains 1.

Template Definition Example 5

If your template definition has the following rules:

```
Image:Image Version:contains:1

OR:Flash File:Size (MB)
```

This custom report is generated with the FlashFile size and Image version of all selected devices. The OR condition without criteria means all flash device sizes.

Template Definition Example 6

If your template definition is the following:

```
Interface:Type:equals:gigabitEthernet
```

```
OR:Interface:Type:contains:voiceFXS
```

This custom report is generated with Interface types of the devices which have interfaces of type gigabitEthernet or voiceFXS.

Template Definition Example 7

If your template definition has the following rules:

```
UDF:user_defined_field_2:contains:xyz
```

```
OR:Flash Device:Total Flash Device Size (MB):>:45
```

This custom report is generated with user_defined_field_2 and Total Flash Device Size (MB) for the devices whose Total Flash Device Size is greater than 45MB or whose user_defined_field_2 value contains string xyz.

Template Definition Example 8

If your template definition has the following rules:

```
Chassis:Port Count
```

```
AND:IP Address:IP Address
```

```
AND:Processor:NVRAM Used (KB)
```

```
AND:Processor:Port Count
```

```
AND:Processor:RAM Size (MB)
```

```
AND:System:Description
```

```
AND:Interface:Type
```

```
OR:UDF:user_defined_field_2
```

```
AND:Flash Partition:Free (KB)
```

This custom report is generated for all given attributes for the selected devices. If any attribute is not collected from the device or if the attribute is not applicable for any device “N/A” will be displayed in the report.

Template Definition Example 9

If your template definition has the following rules:

```
Memory:Type:equals:Processor Memory
```

```
AND:Memory:Type:equals:I/O
```

This custom report is generated for the devices which have both Processor memory and I/O memory.

Template Definition Example 10

If your template definition has the following rules

```
Memory:Type:equals:Processor Memory

AND:Memory:Type:equals:I/O Memory

OR:Memory:Type:equals:Other

AND:Memory:Type:equals:Processor Memory

AND:Memory:Size
```

This custom report is displayed for memory types and memory size of the devices which have either Processor Memory & I/O Memory or Other and Processor Memory.

Template Definition Example 11

If you want to see memory size of the devices located in Bangalore, Chennai and San Jose, the template can be defined as followed.

```
System:Location:equals:Banglore

or:System:Location:equals:Chennai

or:System:Location:equals:SJ

AND:Memroy:Size(MB):equals:ALL
```

Template Definition Example 12

If your template definition has the following rules:

```
UDF:user_defined_field_0:contains:xyz

AND:UDF:user_defined_field_3
```

The custom report is generated for user_defined_field_0 and user_defined_field_3 for devices whose user_defined_field_0 contains string xyz.

For information on cwcli invreport command, see the cwcli section: CLI Utilities, topic: Using the cwcli inventory Command

Using Device Center for Inventory Tasks

The CiscoWorks Common Services Device Center provides a “device-centric” view for CiscoWorks applications and offers you device-centric features and information from one single location.

To access Device Center:

Step 1 Go to the CiscoWorks LMS Portal home page and select **Device Troubleshooting > Device Center**.

The Device Center window appears with the device selector on the right and Device Center overview information on the left section of the screen.

Step 2 Enter the IP address or device name of the device you want to select and click **Go** in the Device Selector field

Or

Select a device from the list-tree.

The Device Summary and Functions Available panes appear in the right section of the screen.

Step 3 Click any of the links under the **Functions Available** pane to launch the corresponding application function.

The links are launched in a separate window.

If you enter the device name or IP address of a device not managed by any of the applications installed on the Common Services server, the Functions Available pane will display only the default connectivity tools from Common Services.

For Inventory application, you can:

- Launch the Detailed Device Report:

  In the Functions Available pane, select **Reports > Detailed Device Report**. For details of this reports, see Generating a Detailed Device Report**.**

- Update Inventory.

  In the Functions Available pane, select **Management Tasks > Update Inventory**.

  This message appears:

  ```
  Successfully created job 1045 for updating inventory.
  Go to Resource Manager Essentials > Devices > Inventory > Inventory Jobs to see
  details.
  ```

  For details of the Inventory Job Browser, see Using the Inventory Job Browser.

CHAPTER 7

Generating Reports

You can perform all your reporting related tasks from a single location—The Reports tab (**Resource Manager Essentials > Reports**).

These tasks are:

- Running reports, both system-defined or user defined, and graphs. See Using the Reports Generator.
- Creating and managing custom reports across applications such as Syslog and Inventory. See Defining Custom Report Templates.
- Managing report jobs. You can view the output for completed jobs, abort or delete jobs, etc. See Using the Reports Job Browser.
- Managing report archives. You can view an archived report. A report is archived when a scheduled report job is completed successfully. See Viewing Archived Reports.
- Performing administrative tasks. You can do administrative operations on reports such as purging the archives, or report jobs. See Purging Reports Jobs and Archived Reports.

Note You can select the log level settings for the Reports application using the feature Application Log Level Settings (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

For the new features in this release, see What's New in this Release.

Using the Reports Job Browser

You can manage report jobs using the Reports job browser. You can also view the output of completed jobs, stop running jobs or delete jobs if required.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To open the Reports Job Browser, select **Resource Manager Essentials > Reports > Report Jobs**.

The Reports Job Browser dialog box appears with a detailed list of all scheduled report jobs.

The columns in the Reports Job Browser dialog box are:

Column	Description
Job ID	Unique ID assigned to the job by the system, when the job is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Job Type	Reporting application—Audit Trail, Bug Toolkit, Change Audit, Contract Connection, Inventory, Syslog, etc.
Report Type	Name of the report.
Status	Status of the scheduled job—Scheduled, Success, Failed, Running, and Cancelled.
Description	Description of the job provided by the job creator. (Alphanumeric characters).
Owner	Username of the job creator.
Scheduled at	Date and time the job was scheduled at.
Completed at	Date and time the job was completed at.
Schedule Type	Specifies the type of schedule for the job: • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. **Note** Report jobs with the Schedule Type Immediate are not displayed in the Reports Job Browser. They are displayed immediately after they are created in separate browser.

Using the Filter by field in the Report Job Browser, you can filter the jobs displayed in the browser.

You can filter the jobs using any of the following criteria and clicking **Filter**:

Filter Criteria	Description
All	Select All to display all jobs in the job browser
Job ID	Select Job ID and enter the whole or the first part of the Job ID(s) that you want to display.

Filter Criteria	Description
Job Type	Select Job Type and then select any one of the following: • Syslog • Bug Toolkit • Inventory • Change Audit • Contract Connection
Report Type	Select Report Type and enter the report name.
Status	Select Status and then select any one of these: • Schedule • Successful • Failed • Cancelled • Running
Description	Select Description and enter the first few letters or the complete description.
Owner	Select Owner and enter the user ID or the beginning of the user ID.
Schedule Type	Select the schedule type and select any one of these: • Once • 6- Hourly • 12-Hourly • Daily • Weekly • Monthly

You can perform the following tasks on the reports displayed in the Job Browser:

- View the report output—Select a successfully completed job and click **Show Output**. If you select more than one job, the Show Output button will be disabled.
- Stop a running job—Select the job and click **Stop**. You are prompted for a confirmation before the job is stopped. You can select more than one job to stop.
- Delete a job—Select the job and click **Delete**. You are prompted for a confirmation before the job is deleted. You can select more than one job to delete.

Refresh (Icon)	Click on this icon to refresh the Reports Job Browser.

Using the Reports Generator

Using the Report Generator of RME, you can generate various reports for these RME applications:

- Audit Trail
- BugToolkit
- Change Audit
- Contract Connection
- Device Credential
- Inventory
- Syslog

You can generate 24-hour reports that show data for the past 24 hours, from the scheduled time of the report.

Successfully generated reports are stored in the Archives. You can access the reports archives by selecting **Resource Manager Essentials >Reports > Report Archives** (see Viewing Archived Reports.)

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To use the Report Generator:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box and select the application for which you want to generate a report.

Step 3 Select a Report. (This selection will not be available if you do not select an application before selecting a Report.)

The RME Reports dialog box appears for the selected report.

Step 4 Select either:

- Device Selector, if you want to schedule report generation for static set of devices.

Or

- Group Selector, if you want to schedule report generation for dynamic group of devices.

The report is scheduled only for the devices that are present in the selected group at the time of report generation. The customizable group selector for reports evaluates static groups also as dynamic during run time.

The RME Reports dialog box appears for the selected report. For details of how to enter information, see the respective chapters or sections in the User Guide.

To generate:

- Syslog Reports, see the topic Overview: Syslog Analyzer Reports in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector.
- Audit Trail Report, see the topic Generating a Standard Audit Trail Report, in the section Tracking RME Server Changes Using Audit Trail.
- BugToolkit Report, see Checking Bug Status Using Bug Toolkit.

- Change Audit Reports, see the topic Tracking Network Changes Using Change Audit, in the section Tracking Network Changes Using Change Audit.
- Inventory Reports, see the topic Generating Inventory Reports in the section Managing Inventory Collection and Polling Using Inventory.
- Contract Connection Reports, see the topic Accessing and Using Contract Connection, in the section Working With Contract Connection.
- Device Credential Reports, see the topic Generating Device Credentials Report.

If you want to reset the information that you have entered into the RME Reports dialog box, and bring the default report settings back, click **Reset**.

Step 5 Click **Finish**.

The report is generated.

Defining Custom Report Templates

The Custom Templates option lets you create a custom template, and edit or delete existing custom templates for Syslog and Inventory applications.

When you select **Resource Manager Essentials > Reports > Custom Reports Templates**, a list of all Custom Templates, appears in the dialog box on the Custom Templates page.

The columns in the Custom Templates dialog box are:

Column	Description
Template Name	Name of the template.
Report Type	Syslog report, or Inventory report.
Owner	User who created the template.
Last Modified Time	Date (yyyy-mm-dd) and the time (hh:mm:ss) the report was last modified.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Using the Custom Templates dialog box, you can do the following tasks:

Task	Button
Create a custom template (see Creating a Custom Report Template).	Create
Edit a custom template (see Editing a Custom Report Template).	Modify
Delete a custom template (see Deleting a Custom Report Template).	Delete

Creating a Custom Report Template

To create a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The Custom Templates dialog box appears with a list of all templates, see Defining Custom Report Templates.

Step 2 Click **Create**.

The Application Selection dialog box appears.

Step 3 Select the required application—Syslog, or Inventory.

Step 4 Click **Next**.

The dialog box for the selected application appears. For details see:

- Syslog custom reports—The topic Defining Custom Report Templates in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector
- Inventory custom reports—The topic Using Inventory Custom Report Templates in the section Managing Inventory Collection and Polling Using Inventory.

Editing a Custom Report Template

To edit a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The Custom Templates dialog box appears.

Step 2 Select the required custom template and click **Modify**.

The Custom Report Template dialog box for the selected application appears.

Step 3 Make the required modifications. For details see:

- Syslog custom reports—The topic Defining Custom Report Templates in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector
- Inventory custom reports—The topic Using Inventory Custom Report Templates in the section Managing Inventory Collection and Polling Using Inventory.

Step 4 Click **Finish**.

Deleting a Custom Report Template

To delete a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The Custom Templates dialog box appears.

Step 2 Select the required report and click **Delete**.

You are prompted to confirm the deletion. If you confirm the deletion, the custom report template is deleted and does not appear in the Custom Report Template dialog box.

Viewing Archived Reports

The report output that is created from a scheduled report is stored in the reports archive. The archive displays the list for completed report jobs and you can view or delete them.

The archive holds the report output even if the report job does not exist.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To view or delete archived reports:

Step 1 Select **Resource Manager Essentials > Reports > Report Archives**.

The Archives dialog box displays all the archived reports.

The columns in the archives dialog box are:

Column	Description
Report Type	Type of archived report—Syslog Report, Inventory report, Bug Toolkit report, etc.
Description	Description of the report, that was entered at creation time.
Creation Time	The date (yyyy-mm-dd) and the time (hh:mm:ss) the report was created.

Step 2 Select the required report.

Step 3 Click **View**.

The archived report that you selected, appears.

If you want to delete an archived report, select the report and click **Delete**.

You are prompted to confirm the deletion.

In the case of Inventory report jobs, when you delete an Inventory report job from the archive, the published report is not deleted from the stored location.

Using the Filter by field in the Report Job Browser, you can filter the jobs displayed in the browser.

You can filter the jobs using any of the following criteria and clicking **Filter**:

Filter Criteria	Description
All	Select All to display all jobs in the job browser

Filter Criteria	Description
Report Type	Select Report Type and enter the report name.
Description	Select Description and enter the first few letters or the complete description.

Refresh (Icon)	Click on this icon to refresh the Archives dialog box.

Note Immediate Run Type reports are not archived.

Purging Reports Jobs and Archived Reports

You can enable a background periodic report job to purge report jobs or reports.

By default, purge is disabled. However, you can create jobs to purge archived reports or report jobs.

After you create a purge job, you can:

- Disable it or enable it, using the Disable or Enable buttons.
- Do an immediate purge operation by clicking **Purge Now**.

For more details about these buttons, see the topic Job Purge in the section Setting System-wide Parameters Using System Preferences

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To enable the purge option for reports and report jobs:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears. For details about the fields in this dialog box, see the topic Job Purge in the section Setting System-wide Parameters Using System Preferences.

Step 2 In the Application column of the Job Purge dialog box, select either of these options:

- Reports Jobs

  or

- Reports Archive Purge

Step 3 Click **Schedule**.

The Purge Schedule dialog box appears.

The fields in the Purge Schedule dialog box are:

Field	Description
Scheduling	
Run Type	Specifies the type of schedule for the job: • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. (A month comprises 30 days). For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	1. Click on the date picker icon and select the date, month and year. Your selection appears in the Date field in this format: ddMmmyyyy (example: 14 Nov 2004). 2. Select the time (hh and mm) from the drop-down lists in the **at** fields.
Job Info	
Days	The default setting for purging both archived reports and report jobs is 180 days. That is, reports or report jobs older than 180 days will be purged. You can change value this as required. This is a mandatory field.
Job Description	Based on the option that you selected, one of these default job descriptions appears: • Purge - Reports Archive Purge or • Purge - Reports Jobs
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses, separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter your comments for the purge job that you are scheduling.

Step 4 Click **Done** to save your changes.

Setting the Reports Archive Default Directory

You can use the Archive Settings window to change the default directory location for reports archival on the RME server.

The default Reports Archive directory is:

On RME Solaris server,

`/var/adm/CSCOpx/files/rme/cri`

On RME Windows server,

NMSROOT`\files\rme\cri`

Where *NMSROOT* is the CiscoWorks installed directory.

The new default directory location specified by you should have the permission for *casuser*:*casusers* in Solaris and *casuser* should have Full Control in Windows.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The following is the workflow for changing the default directory for reports archive :

Step 1 Go to **Resource Manager Essentials** > **Admin** > **Reports** > **Archive Settings**.

The Archive Settings dialog box appears.

Step 2 Enter the new location in the Archive Location field, or click **Browse** to select a directory on your system.

Step 3 Either Click on **Apply** to accept the change to directory or **Cancel** to revert back to the previous default directory location.

If you had clicked on **Apply**, a message appears confirming the changes.

CHAPTER 8

Archiving Configurations and Managing Them Using Archive Management

The Archive Management application maintains an active archive of the configuration of devices managed by RME. It enables you to perform the following tasks:

- Fetch, archive, and deploy device configurations.
- Search and generate reports on archived data
- Compare and label configurations, compare configurations with a baseline, and check for compliance.

You can also perform some of the Archive Management tasks using command line utility **`cwcli config`**.

You can also export the configuration data using the **`cwcli export config`** command. See CLI Utilities for further details on **`cwcli config`** and **`cwcli export config`** commands.

This chapter gives information on performing:

- Archive Management tasks (see Archive Management allows you to: for details).
- Archive Management administrative tasks (see Performing Archive Management Administrative Tasks for details).
- Configuration Management administrative tasks (see Performing Configuration Management Administrative Tasks for details).

Performing Archive Management Tasks

Archive Management allows you to:

- Update the archive

  In addition to scheduling configuration archive update, you can also update the archive manually. This ensures that you have the latest configurations.

  See Scheduling Sync Archive Job and Defining the Configuration Collection Settings for further details.

- Check archival status

  You can check the overall status of the configuration archive (For example, Successful, Partially Successful, etc.).

  See Checking Configuration Archival Status for further details.

- Determine out-of-sync configuration files

  You can list the devices for which running configurations are out-of-sync- with the startup configuration.

  See Generating an Out-of-Sync Report and Scheduling Sync on Device Job for further details.

- View Version Tree

  You can view all configuration versions of selected devices in the form of a graphical display.

  See Using the Configuration Version Tree for further details.

- View Version Summary

  You can view the latest three archived configurations for selected devices. It also has a link to view a particular configuration running on the device and to generate differences between versions in the archive.

  See Viewing the Configuration Version Summary for further details.

- Search for device configuration files

  You can search the archive for configuration containing text patterns for selected devices.

  See Using Search Archive for further details.

- Create custom configuration queries (See Creating a Custom Query.)

  You can create and run custom queries that generate reports. These reports display device configuration files from the archive for the devices you specify. You can use custom queries while searching archives.

- Compare configurations

  You can compare startup and running configurations, running and latest archived configurations. You can also compare two configuration versions of the same device, or two configuration versions of different devices.

  See Comparing Configuration for further details.

- Configuration Quick Deploy

  You can create an immediate job to deploy the version of configuration that you are viewing on the device. You can deploy the configuration either in the Overwrite or Merge mode. You can also use job-based password.

  See Configuration Quick Deploy for further details.

- Archive Management Job Browser

  You can see the status of your Archive Management jobs.

  See Using Archive Management Job Browser for further details.

- Label Configuration

  You can select configuration files from different managed devices and then group and label them.

  See Configuring Labels for further details.

- Baseline Template

  You can compare the baseline template with the configuration of devices in the archive. You can also generate a non-compliance configuration report and deploy this template onto the devices to make it compliant.

  See Baseline Template for further details.

- Set the debug mode for Archive Management application

You can set the debug mode for Archive Management application in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

See Application Log Level Settings for further details.

- Using Device Center you can perform these Archive Management tasks:
  - Viewing the latest configuration archived details
  - Viewing the differences between the two archived running configuration
  - Updating the configuration archive

  See RME Device Center for further details.

Performing Archive Management Administrative Tasks

The administrative tasks for Archive Management are:

- Modify configuration collection and polling settings

  You can enable or disable the configuration collection and polling tasks. You can also schedule a periodic job for configuration collection and polling.

  See Defining the Configuration Collection Settings for further details.

- Move the configuration archive directory (See Moving the Configuration Archive Directory.)

  You can move the configuration archive directory to a new location.

- Enable and disable the Shadow directory (See Enabling and Disabling the Shadow Directory.)

  You can enable or disable the use of the Shadow directory.

  The configuration archive Shadow directory is an image of the most recent configurations gathered by the configuration archive. You can use the shadow directory as an alternative method to get the latest configuration information programmatically, using scripts or other means.

- Configure Exclude Commands (See Configuring Exclude Commands.)

  You can list the commands that have to be excluded while comparing configuration.

- Purge configurations files from the archive (See Purging Configurations from the Configuration Archive.)

  You can enable or disable the purge task and also modify the schedule. This frees disk space and maintains your archive at a manageable size.

You need to set up your devices for the configuration archive. See Preparing to Use the Archive Management.

Performing Configuration Management Administrative Tasks

The administrative tasks for configuration Management (applicable to Archive Management, Config Editor, `cwcli config`, and NetConfig) are:

- Configure Transport Protocol (See Configuring Transport Protocols.)

  You can set the transport protocol order for Archive Mgmt, NetConfig, and Config Editor jobs.

- Config Job Policies (See Configuring Default Job Policies.)

You can enable the job password policy for Archive Mgmt, NetConfig, Config Editor, and `cwcli config`. You can also configure the default job policies if the job fails.

For the new features in this release, see What's New in this Release.

Preparing to Use the Archive Management

Before you start using the Archive Management, you must:

- Enter Device Credentials (See Entering Device Credentials for details)
- Modify Device Configurations (See Modifying Device Configurations for details)
- Modify Device Security (See Modifying Device Security for details)

Entering Device Credentials

Enter the following device credentials in the Device and Credentials window (**Common Services > Device and Credentials > Device Management**):

- Read and write community strings
- Primary Username and Password
- Primary Enable Password

If you have enabled the Enable Job Password option in the Config Job Policy dialog box ((**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) when you scheduled the Config jobs, you are prompted for the following device credentials:

- Login User name
- Login Password
- Enable Password

The supported Device authentication prompts are:

- Routers

  "Username:", "Username: "

  "Password:", "Password: "

- Switches

  "username: ", "Username: "

  "password: ", "Password: "

- Cisco Interfaces and Modules—Network Analysis Modules

  "login: "

  "Password: " "password: "

- Security and VPN—PIX

  "username: ", "Username: "

  "passwd: ", "password: ", "Password: "

- Content Networking—Content Service Switch

  "Username: ", "username: ", "login: ","Username:" , "username:" , "login:"

“Password: ”, “password: ”, “passwd: ”,”Password:” , “password:” , “passwd:”

- Content Networking—Content Engine

  “Username: ” ,”login: ”

  “Password: ”

- Storage Networking—MDS Devices

  “Username:”, “Username: ”

  “Password:”, “Password: ”

Note If you enabled TACACS for a device and configured custom TACACS login and passwords prompts, you may experience Telnet problems, since RME may not recognize the prompts. To make your prompts recognizable, you must edit the TacacsPrompts.ini file. See the procedure given in the Handling Custom Telnet Prompts section of the User Guide for Common Services.

Modifying Device Configurations

To enable the configuration archive to gather the configurations, modify the device configurations for the following:

- Enabling rcp
- Enabling scp
- Enabling https
- Configuring Devices to Send Syslogs

Enabling rcp

To enable the configuration archive to gather the configurations using the rcp protocol, modify your device configurations.

Make sure the devices are rcp-enabled by entering the following commands in the device configurations:

```
# ip rcmd rcp-enable
# ip rcmd remote-host local_username {ip-address | host} remote_username [enable]
```

Where *ip_address* | *host* is the IP address/hostname of the machine where RME is installed. Alternatively, you can enter the hostname instead of the IP address. The default *remote_username* and *local_username* are `cwuser`.

Disable the DNS security check for rcp if your RME server and devices are not registered with the DNS server. To do this, use the command, `no ip rcmd domain-lookup` for rcp to fetch the device configuration.

Enabling scp

To enable the configuration archive to gather the configurations using the scp protocol, modify your device configurations.

To configure local User name:

```
aaa new-model
aaa authentication login default local

aaa authentication enable default none

aaa authorization exec default local


username admin privilege 15 password 0 system

ip ssh authentication-retries 4

ip scp server enable
```

To configure TACACS User name:

```
aaa new-model

aaa authentication login default group tacacs+

aaa authentication enable default none

aaa authorization exec default group tacacs+


ip ssh authentication-retries 4

ip scp server enable
```

User on the TACACS Server should be configured with priv level 15:

```
user = admin {

        default service = permit

        login = cleartext "system"

        service = exec {

                priv-lvl = 15

        }

}
```

Enabling https

To enable the configuration archive to gather the configurations using https protocol you must modify your device configurations.

To modify the device configuration, follow the procedure as described in this URL:

http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1d98.html#999607

Configuring Devices to Send Syslogs

Configure your devices for Syslog Analysis if you want the device configurations to be gathered and stored automatically in the configuration archive when Syslog messages are received.

After you perform these tasks and the devices become managed, the configuration files are collected and stored in the configuration archive.

Modifying Device Security

Configuration Management must be able to run certain commands on devices to archive their configurations.

You must disable security on the devices, the configurations of which you want to archive. This is because the security on the device prohibits Configuration Management from running these commands:

- Router Commands
- Switches Commands
- Content Networking—Content Service Switch Commands
- Content Networking—Content Engine Commands
- Cisco Interfaces and Modules—Network Analysis Modules
- Security and VPN—PIX Devices

Router Commands

Command	Description
`terminal length 0`	Sets the number of lines on the current terminal screen for the current session
`terminal width 0`	Sets the number of character columns on the terminal screen for the current line for a session
`show privilege`	Displays your current level of privilege
`Show running`	Gets running configuration.
`Show startup`	Gets startup configuration
`Show running-brief`[1]	Gets the running configuration in brief by excluding the encryption keys.

[1] This is applicable for the IOS release 12.3(7)T release or later.

The commands in the above tables also apply to the following device types:

- Universal Gateways and Access Servers
- Universal Gateways and Access Servers
- Optical Networking
- Broadband Cable
- Voice and Telephony
- Wireless
- Storage Networking

Switches Commands

The switches commands are:

Command	Description
`set length 0`	Configures the number of lines in the terminal display screen
`set logging session disable`	Disables the sending of system logging messages to the current login session.
`write term`	Gets running configuration.

Content Networking—Content Service Switch Commands

The Content Service Switch commands are:

Command	Description
`no terminal more`	Disables support for more functions with the terminal.
`show running-config`	Gets all components of the running configuration.
`show startup-config`	Gets the CSS startup configuration (startup-config).

Content Networking—Content Engine Commands

The Content Engine commands are:

Command	Description
`terminal length 0`	Sets the number of lines on the current terminal screen for the current session
`show run`	Gets running configuration.
`show config`	Gets startup configuration.

Cisco Interfaces and Modules—Network Analysis Modules

The Network Analysis Modules commands are:

Command	Description
`terminal length 0`	Sets the number of lines on the current terminal screen for the current session
`show autostart`	Displays autostart collections
`show configuration`	Gets startup configuration.

Security and VPN—PIX Devices

The PIX devices commands are:

Command	Description
`terminal width 0`	Sets the number of character columns on the terminal screen for the current line for a session
`show config`	Gets startup configuration.
`show running`	Gets running configuration.
`show curpriv`	View the current logged-in user.
`no pager`	Removes paging control

Using Job Approval for Archive Management

You can enable Job Approval for Archive Management tasks, (**Resource Manager Essentials > Admin > Approval > Approval Policies**). This means all jobs require approval before they can run.

Only users with Approver permissions can approve Archive Management jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

For more details on enabling job approval see Setting Up Job Approval in the section Enabling Approval and Approving Jobs Using Job Approval.

The following Archive Management tasks require approval if you have enabled Job Approval:

- Out-of-Sync (**Config Mgmt > Archive Mgmt > Out-of-Sync Summary**)
- Deploy (**Config Mgmt > Archive Mgmt > Baseline Templates** and **Config Mgmt > Archive Mgmt > Baseline Templates > Compliance**)
- Compliance Check (**Config Mgmt > Archive Mgmt > Baseline Templates > Compliance**)

  This is only if you enable the Check Compliance and Deploy option in the Job Schedule and Options dialog box.

Sync Archive jobs do not have Job Approval enabled because this job only archives the configuration from the device and there is no change to the device configuration.

If you have enabled Approval for Archive Management tasks, then in the Job Schedule and Options dialog box, you get these options:

- Approval Comment—Approval comments for the job approver.
- Maker E-Mail—E-mail-id of the job creator.

Configuring Transport Protocols

You can set the protocol order for Configuration Management applications such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations. For NetShow, you can set the protocol order to download configurations.

This setup allows you to use your preferred protocol order for fetching and downloading the configuration.

The available protocols are:

- Telnet
- TFTP (Trivial File Transport Protocol)

- rcp (remote copy protocol)
- SSH (Secure Shell)
- SCP (Secure Copy Protocol)
- HTTPS (Hyper Text Transfer Protocol Secured)

Requirements to Use the Supported Protocols

If the following requirements are not met, an error message appears.

To use this Protocols	You must...
Telnet	Know Telnet passwords for login and Enable modes for device. If device is configured for TACACS authentication, enter Primary Username and Primary Password.
TFTP	Know read and write community strings for device.
rcp	Configure devices to support incoming rcp requests. To make sure the device is rcp-enabled, enter the following commands in the device configuration: # **`ip rcmd rcp-enable`** # **`ip rcmd remote-host`** *local_username* {*ip-address* | *host*} *remote_username* [**`enable`**] where *ip_address* | *host* is the IP address/hostname of the machine where RME is installed. The default *remote_username* and *local_username* are *cwuser*. For example, you can enter: # **`ip rcmd remote-host`** *cwuser 123.45.678.90 cwuser* **`enable`** **Note** Disable the DNS security check for rcp if your RME server and devices are not registered with the DNS server. To do this, use the command, **`no ip rcmd domain-lookup`** for rcp to fetch the device configuration.

To use this Protocols	You must...
SSH	Know the username and password for the device. If device is configured for TACACS authentication, enter the Primary Username and Primary Password. Know password for Enable modes. When you select the SSH protocol for the RME applications (Configuration Archive, NetConfig, ConfigEditor, and NetShow) the underlying transport mechanism checks whether the device is running SSHv2. If so, it tries to connect to the device using SSHv2. If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1. If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2. If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed. Some useful URLs on configuring SSHv2 are: • Configuring Secure Shell on Routers and Switches Running Cisco IOS: http://www.cisco.com/warp/public/707/ssh.shtml • How to Configure SSH on Catalyst Switches Running Catalyst OS: http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a0080094314.shtml • Configuring the Secure Shell Daemon Protocol on CSS: http://www.cisco.com/en/US/partner/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a00801eea45.html#1105358 • Configuration Examples and TechNotes: – http://www.cisco.com/en/US/tech/tk583/tk617/tech_configuration_examples_list.html – http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802045dc.html

To use this Protocols	You must...
SCP	Know the SSH username and password for the device. To make sure the device is scp-enabled, enter the following commands in the device configuration. To configure local User name:

```
aaa new-model
aaa authentication login default local
aaa authentication enable default none
aaa authorization exec default local

username admin privilege 15 password 0 system
ip ssh authentication-retries 4
ip scp server enable
```

To configure TACACS User name:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authentication enable default none
aaa authorization exec default group tacacs+

ip ssh authentication-retries 4
ip scp server enable
```

User on the TACACS Server should be configured with privilege level 15:

```
user = admin {
        default service = permit
        login = cleartext "system"
        service = exec {
                priv-lvl = 15
        }
}
```

To use this Protocols	You must...
HTTPS	Know the username and password for the device. Enter the Primary Username and Password in the Device and Credential Repository (Common Services > Device and Credentials > Device Management). To enable the configuration archive to gather the configurations using https protocol you must modify your device configurations: http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1d98.html#999607 This is used for VPN 3000 device.

The configuration archive uses Telnet/SSH to gather the module configurations of Catalyst 5000 family devices and vlan.dat file in case of Catalyst IOS switches. Make sure you enter the correct Telnet and Enable passwords.

If you enabled TACACS for a device and configured custom TACACS login and passwords prompts, you may experience Telnet problems, since RME may not recognize the prompts. To make your prompts recognizable, you must edit the TacacsPrompts.ini file. See the procedure given in the Handling Custom Telnet Prompts section of the User Guide for Common Services.

For module configs, the passwords on the module must be same as the password on the supervisor.

Supported Protocols for Configuration Management Applications

For supported protocol at individual device-level, you can either see:

- The RME device packages Online help. You can launch the RME device packages Online help using **Help > Resource Manager Essentials > Device Packages**.

  or

- The Supported Protocols for Configuration Management table on Cisco.com:

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baa8.html

Defining the Protocol Order

The following is the workflow for defining the protocol order for Configuration Management applications to perform either Config fetch or Config update:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt**.

The Config Transport Settings dialog box appears.

Step 2 Go to the first drop-down list box, select the application for which you want to define the protocol order.

Step 3 Select a protocol from the Available Protocols pane and click **Add**.

If you want to remove a protocol or change the protocol order, you must remove the protocol using the **Remove** button and add the protocol, again.

The list of protocols that you have selected appears in the Selected Protocol Order pane.

When a configuration fetch or update operation fails, an error message appears. This message displays details about the supported protocol for the particular device and it modules, if there are any.

For the list of supported protocols, see Supported Device Table for Configuration Management application on Cisco.com.

Step 4 Click **Apply**.

A message appears, `New settings saved successfully`.

Step 5 Click **OK**.

Configuring Default Job Policies

Each Configuration Management job has properties that define how the job will run. You can configure a default policy for these properties that applies to all future jobs. You can also specify for each property whether users can change the default when creating a job.

You have the option of entering a username and password for running a specific Archive Management, Config Editor, NetConfig, or NetShow job.

If you enter a username and password, Archive Management, Config Editor, or NetConfig applications use this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository.

While the job is running, the password is retrieved from the Device and Credential Repository for each of the selected devices.

For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Device and Credential Repository should be synchronized (with every password change).

This option of entering the username and password for running a job is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

To use this option of entering a username and password for running a specific job, you should enable the job password policy for Archive Management, Config Editor, NetConfig, or NetShow jobs.

You can do this by using the Enable Job Password option in the Config Job Policies window.

If you have enabled Enable Job Password option, you can enter these credentials while scheduling a job:

- Login Username
- Login Password
- Enable Password

Defining the Default Job Policies

The following is the workflow for defining the default job policies for Configuration Management applications:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Config Job Policies**.

The Job Policy dialog box appears.

Step 2 Select the applications.

Step 3 Based on your selection, enter the following information:

Field Name	Description	Usage Notes
Failure Policy This appears only if you select either Config Editor or NetConfig application.	Select what the job should do if it fails to run on the device. You can stop or continue the job, and roll back configuration changes to the failed device or to all devices configured by the job. You can select one of the options: • Stop on failure—Stops the job on failure. • Ignore failure and continue—Continues the job on failure. • Rollback device and stop—Rolls back the changes on the failed device and stops the job. This is applicable only to NetConfig application. • Rollback device and continue—Rolls back the changes on the failed device and continues the job. This is applicable only to NetConfig application. • Rollback job on failure—Rolls back the changes on all devices and stops the job. This is applicable only to NetConfig application.	You can create rollback commands for a job in the following ways: • Using a system-defined template. Rollback commands are created automatically by the template. The Banner system-defined template does not support rollback. You cannot create rollback commands using this template. • Creating a user template. Allows you to enter rollback commands into the template. When you use the Adhoc and Telnet Password templates, you cannot create rollback commands.
E-mail Notification This appears for all the applications in the dropdown list.	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.	Notification is sent when the job is started and completed. Notification E-mails include a URL to enter to display job details. If you are not logged in, do so using log in panel.

Field Name	Description	Usage Notes
Sync Archive before Job Execution This appears if you select either Config Editor or NetConfig application.	The job archives the running configuration before making configuration changes.	None.
Copy Running Config to Startup This appears if you select either Config Editor or NetConfig application.	The job writes the running configuration to the startup configuration on each device after configuration changes are made successfully.	Does not apply to Catalyst OS devices.
Enable Job Password This appears for all the applications in the dropdown list.	The job Password Policy is enabled for all the jobs. The Archive Management, Config Editor, and NetConfig jobs use this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository. These device credentials are entered while scheduling a job.	None. You can use this option even if you have configured only the Telnet password (without configuring username) on your device. You must enter a string in the Login Username field. Do not leave the Login Username field blank. The Login Username string will be ignored while connecting to the device since the device is configured only for the Telnet password. See Usage Scenarios When Job Password is Configured on Devices.
Fail on Mismatch of Config Versions This appears if you select either Config Editor or NetConfig application.	The job is considered a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.	None.
Delete Config after download This appears if you select Config Editor.	The configuration file is deleted after the download.	

Field Name	Description	Usage Notes
Execution Policy This appears for all the applications in the dropdown list.	Allows you to configure the job to run on multiple devices at the same time (Parallel execution) or in sequence (Sequential Execution).	If you select sequential execution, you can select Device Order in the Job Schedule and Options dialog box to set the order of the device. 1. Select a device in the Set Device Order dialog box. 2. Either: • Click the Move Up or Move Down arrows to change its place in the order. Click **Done** to save the current order. Or • Close the dialog box without making any changes. You cannot alter the device sequence for Archive Management application jobs such as Sync Archive, Check Compliance and Deploy, etc. Sequential Execution is not supported for the following jobs: • Manual Sync Archive • Periodic Config Collection and Polling • cwcli config get
User Configurable	Select this check box next to any field to make corresponding policy user configurable.	You can configure a user-configurable policy while defining job. You cannot modify non-user-configurable policies.

Step 4 Click **Apply**.

A message appears, `Policy values changed successfully`.

Step 5 Click **OK**.

Usage Scenarios When Job Password is Configured on Devices

The following tables list the usage scenarios and their implications for Configuration application when job password is configured on devices.

- Table 8-1When Device Access is Only Through Job Password and No Access is Available Through Regular Telnet/SSH and SNMP (Read or Write)
- Table 8-2When Devices are Configured for Job Password and Access is Available Through SNMP (Read or Write)
- Table 8-3When Devices are not Configured for Job Password and Access is Available Through Regular Telnet/SSH but no SNMP
- Table 8-4When Devices are not Configured for Job Password and Regular Telnet/SSH is Disabled. Access is Available Only Through SNMP (Read or Write)

Table 8-1 When Device Access is Only Through Job Password and No Access is Available Through Regular Telnet/SSH and SNMP (Read or Write)

Scenario	**Archive Mgmt**	**cwcli config**	**NetConfig**	**Config Editor**
Device is added into RME	Fails	Not applicable	Not applicable	Not applicable
Update archive request through user interface	Fails	Not applicable	Not applicable	Not applicable
Update archive request through command line	Not applicable	Fails	Not applicable	Not applicable
Config update when Syslog message is received	Fails	Not applicable	Not applicable	Not applicable
Config update through periodic scheduled process	Fails	Not applicable	Not applicable	Not applicable
Config update through SNMP poller based scheduled process	Fails	Not applicable	Not applicable	Not applicable
Config upload/restore through `cwcli config`	Not applicable	Fails	Not applicable	Not applicable
NetConfig Job	Not applicable	Fails	Succeeds	Not applicable
Config Editor job	Not applicable	Not applicable	Not applicable	Succeeds

Table 8-2 When Devices are Configured for Job Password and Access is Available Through SNMP (Read or Write)

Scenario	**Archive Mgmt**	**cwcli config**	**NetConfig**	**Config Editor**
Device is added into RME	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Update archive request through user interface	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Update archive request through command line	Succeeds for SNMP supported devices	Succeeds for SNMP supported devices	Not applicable	Not applicable
Config update when Syslog message is received	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Config update through periodic scheduled process	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Config update through SNMP poller based scheduled process	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Config upload/restore through `cwcli config`	Not applicable	Succeeds for SNMP supported devices	Not applicable	Not applicable

Table 8-2 When Devices are Configured for Job Password and Access is Available Through SNMP (Read or Write)

Scenario	Archive Mgmt	cwcli config	NetConfig	Config Editor
NetConfig Job	Not applicable	Fails	Succeeds	Not applicable
Config Editor job	Not applicable	Not applicable	Not applicable	Succeeds

Table 8-3 When Devices are not Configured for Job Password and Access is Available Through Regular Telnet/SSH but no SNMP

Scenario	Archive Mgmt	cwcli config	NetConfig	Config Editor
Device is added into RME	Succeeds	Not applicable	Not applicable	Not applicable
Update archive request through user interface	Succeeds	Not applicable	Not applicable	Not applicable
Update archive request through command line	Succeeds	Succeeds	Not applicable	Not applicable
Config update when Syslog message is received	Succeeds	Not applicable	Not applicable	Not applicable
Config update through periodic scheduled process	Succeeds	Not applicable	Not applicable	Not applicable
Config update through SNMP poller based scheduled process	Succeeds	Not applicable	Not applicable	Not applicable
Config upload/restore through **`cwcli config`**	Succeeds	Succeeds	Not applicable	Not applicable
NetConfig Job	Not applicable	Not applicable	Succeeds	Not applicable
Config Editor job	Not applicable	Not applicable	Not applicable	Succeeds

Table 8-4 When Devices are not Configured for Job Password and Regular Telnet/SSH is Disabled. Access is Available Only Through SNMP (Read or Write)

Scenario	Archive Mgmt	cwcli config	NetConfig	Config Editor
Device is added into RME	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Update archive request through user interface	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Update archive request through command line	Succeeds for SNMP supported devices	Succeeds for SNMP supported devices	Not applicable	Not applicable
Config update when Syslog message is received	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable

Table 8-4 When Devices are not Configured for Job Password and Regular Telnet/SSH is Disabled. Access is Available Only Through SNMP (Read or Write) (continued)

Scenario	Archive Mgmt	cwcli config	NetConfig	Config Editor
Config update through periodic scheduled process	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Config update through SNMP poller based scheduled process	Succeeds for SNMP supported devices	Not applicable	Not applicable	Not applicable
Config upload/restore through **`cwcli config`**	Succeeds for SNMP supported devices	Succeeds for SNMP supported devices	Not applicable	Not applicable
NetConfig Job	Not applicable	Fails	Fails	Not applicable
Config Editor job	Not applicable	Not applicable	Not applicable	Fails

Setting Up Archive Management

You can move the directory for archiving the RME device configuration and enable and disable the usage of Shadow directory. You can also list the commands that need to be excluded while comparing configuration

To do this select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt**.

- Moving the Configuration Archive Directory
- Enabling and Disabling the Shadow Directory
- Configuring Exclude Commands

Moving the Configuration Archive Directory

You can move the directory where the configuration of the devices can be archived on the RME server.

The default Configuration Archive directory is:

On RME Solaris server,

`/var/adm/CSCOpx/files/rme/dcma`

On RME Windows server,

NMSROOT`\files\rme\dcma`

Where *NMSROOT* is the CiscoWorks installed directory.

The new location specified by you should have the permission for *casuser*:*casusers* in Solaris and *casuser* should have Full Control in Windows.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The following is the workflow for moving the configuration archive location:

Step 1 Stop the *ConfigMgmtServer* process. To do this:

- **a.** Select **Common Services > Server > Admin > Processes**.

  The Process Management dialog box appears.
- **b.** Select the *ConfigMgmtServer* process.
- **c.** Click **Stop**.

Step 2 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt**.

The Archive Settings dialog box appears.

Step 3 Enter the new location in the Archive Location field, or click **Browse** to select a directory on your system.

Step 4 Click **Apply**.

A message appears confirming the changes.

Step 5 Restart the *ConfigMgmtServer* process. To do this:

- **a.** Select **Common Services > Server > Admin > Processes**.

  The Process Management dialog box appears.
- **b.** Select the *ConfigMgmtServer* process.
- **c.** Click **Start**.

Enabling and Disabling the Shadow Directory

The configuration archive Shadow directory is an image of the most recent configurations gathered by the configuration archive.

The Shadow directory contains subdirectories that represent each device class and the latest configurations supported by the configuration archive.

Each file name is *DisplayName*.cfg, where *DisplayName* is the device's Display Name as defined in the Device and Credential Repository. Each time the archive is updated, the Shadow directory is updated with the corresponding information.

The Shadow directory can be used as an alternative method to derive the latest configuration information programmatically by using scripts or other means.

To access to the Shadow directory, you must be root or casuser on Solaris, or in the administrator group for Windows.

You can find the Shadow directory in the following locations:

- On Solaris, /var/adm/CSCOpx/files/rme/dcma/shadow
- On Windows, *NMSROOT*/files/rme/dcma/shadow. Where *NMSROOT* is the directory in which RME is installed (the default is C:\Program Files\CSCOpx).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You can enable or disable the use of Shadow directory by following this workflow:

Step 1 Stop the *ConfigMgmtServer* process. To do this:

a. Select **Common Services > Server > Admin > Processes**.

   The Process Management dialog box appears.

b. Select the *ConfigMgmtServer* process.

c. Click **Stop**.

Step 2 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt**.

The Archive Settings dialog box appears.

Step 3 Select the Enable Shadow Directory check box.

Step 4 Click **Apply**.

A message shows that the changes were made.

Step 5 Restart the *ConfigMgmtServer* process. To do this:

a. Select **Common Services > Server > Admin > Processes.**

   The Process Management dialog box appears.

b. Select the *ConfigMgmtServer* process.

c. Click **Start**.

Configuring Exclude Commands

You can list the commands that have to be excluded while comparing configuration. To do this select **Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt** > **Exclude Commands**.

You can enter multiple commands separated by commas.

RME provides default exclude commands for some Device Categories.

For example, the default exclude commands for Router device category are,
end,exec-timeout,length,width,certificate,ntp clock-period

You can specify Exclude Commands at all these levels:

- Device Category (For example, Routers, Wireless, etc.)
- Device Family (For example, Cisco 1000 Series Routers, Cisco 1400 Series Routers, etc.)
- Device Type (For example, Cisco 1003 Router, Cisco 1401 Router, etc.)

While comparing configurations, if you have specified exclude commands in the Device Type, Device Family and Device Category, these commands are excluded only at the Device Type level. The commands in the Device Family and Device Category are not excluded.

Example 1:

If you have specified these commands at,

- Routers (Device Category) level

  ```
  end,exec-timeout,length,width,certificate,ntp clock-period
  ```

- Cisco 1000 Series Routers (Device Family) level

  ```
  banner incoming,snmp-server location
  ```

- Cisco 1003 Router (Device Type) level

  `ip name-server,banner motd,snmp-server manager session-timeout`

While comparing configurations, only the Cisco 1003 Router (Device Type) level commands are excluded.

Example 2:

If you have specified these commands only at Device Family and Device Category,

- Routers (Device Category) level

  `end,exec-timeout,length,width,certificate,ntp clock-period`
- Cisco 1000 Series Routers (Device Family) level

  `banner incoming,snmp-server location`
- Cisco 1003 Router (Device Type) level

  No commands specified.

While comparing configurations, only the Cisco 1000 Series Routers (Device Family) level commands are excluded.

If the commands are specified only at the Device Category level, these commands are applicable to all devices under that category.

To configure Exclude Commands:

Step 1 Select **Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Exclude Commands**.

The Configure Exclude Commands dialog box appears.

Step 2 Select one of these from the Device Type Selector pane:

- Device Category (For example, Routers, Wireless, etc.)
- Device Family (For example, Cisco 1000 Series Routers, Cisco 1400 Series Routers, etc.)
- Device Type (For example, Cisco 1003 Router, Cisco 1401 Router, etc.)

Step 3 Enter the command in the Exclude Commands pane to add new commands.

You can enter multiple commands separated by commas.

You can also edit or delete the existing commands in the Exclude Commands pane.

Step 4 Click **Apply**.

A message appears, `The commands to be excluded are saved successfully`.

Configuring Fetch Settings

You can configure the Job Result Wait Time per device for the Sync Archive Jobs. The default value is 120 seconds. The minimum value can be set to 60 seconds.

Job Result Wait Time is the maximum wait time that Archive Management waits to get the configurations from the device during the sync-archive job execution.

To configure the Job Result Wait Time:

Step 1 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt**.

The Fetch Settings dialog box appears.

Step 2 Provide the Job Result wait time in seconds in the Maximum time to wait for Job results per device (seconds) field.

Step 3 Click:

- **Apply**, if you want to submit the Job Result Wait Time entered.
- **Cancel** if you want to cancel the changes made to the Job Result Wait Time.

Understanding Configuration Retrieval and Archival

RME supports five different ways to trigger the retrieval of configuration files from the device for archival purposes.

Schedule Periodic Configuration File Archival

RME will archive both the startup and running configuration files for all devices at the scheduled time (6-hourly, 12-hourly, daily, weekly, monthly), as configured by the user.

Since this method collects the full running configuration and startup configuration files for the entire network, we recommend that you schedule this to run at no more than once per day, especially if the network is large and outside the LAN.

See Defining the Configuration Collection Settings for further details.

Schedule Periodic Configuration Polling

RME can be configured to periodically poll configuration MIB variables on devices that support these MIBs according to a specified schedule, to determine if either the startup or running configuration file has changed.

If it has, RME will retrieve and archive the most current configuration file from the device.

Polling uses fewer resources than full scheduled collection, because configuration files are retrieved only if the configuration MIB variable is set.

On IOS devices the variables *ccmHistoryRunningLastChanged* and *ccmHistoryStartupLastChanged* from the *CISCO-CONFIG-MAN-MIB MIB*, and on CATOS the variable *sysConfigChangeTime* from *CISCO-STACK-MIB* are used to detect the change.

Any change in the value of these variables causes the configuration file to be retrieved from the device. SNMP change polling works only in case of IOS and CATOS devices which support these MIBs.

If these MIBs are not supported on the devices, then by default, configuration fetch will be initiated without checking for the changes.

By default, the Periodic Collection and Polling are disabled.

See Defining the Configuration Collection Settings for scheduling the periodic polling.

Note The Syslog application triggers configuration fetch, if configuration change messages like SYS-6-CFG_CHG, CPU_REDUN-6-RUNNING_CONFIG_CHG etc., are received.

Manual Updates (Sync Archive function)

This feature allows the RME user to force the configuration archive to check specified devices for changes to the running configuration file only. Use Sync Archive if you need it to synchronize quickly with the running configuration.

You can also poll the device and compare the time of change currently on the device with the time of last archival of the configuration to determine whether the configuration has changed on a device.

The Startup configuration is not retrieved during manual update archive operation. However, you can retrieve the Startup configuration by enabling the Fetch startup Config option while scheduling Sync Archive job.

See Scheduling Sync Archive Job for further details.

Using Version Summary

You can trigger a configuration file retrieval by clicking on the Running or Startup configuration in the Configuration Version Summary report.

After a configuration file is fetched from the device, as described above, RME submits the configuration file for archival.

See Viewing the Configuration Version Summary for further details.

Timestamps of Configuration Files

These are timestamps of a running configuration file, or the change time (in change audit), indicate the time at which RME system archived the configuration file.

This is not the time at which the configuration actually changed on the device. If changes are detected immediately using Syslog messages, the timestamp should be very close to the actual configuration change time on the device.

Startup configurations are handled differently by RME. Startup configs are simply saved into the system, as they are retrieved from the device (unlike running configurations, which are compared and saved in versioned archives, if different).

The timestamps of Startup Configuration files are just the archival times, and do not indicate the change time.

In the version summary reports, the Running and Startup are links, which when clicked will retrieve in real time, the respective configuration from the device. This column does not have a timestamp associated with it.

In the Out-Of-Sync report, the Startup configuration column indicates the last archived startup configuration along with its timestamp, and the Running configuration column indicate the last archived running config along with its timestamp.

How Running Configuration is Archived

The workflow for archiving the Running configuration is:

1. If RME detects an effective change, the new configuration is queued for Archival.
2. The archiver, calculates the exact effective changes, assigns a new version number for the newly collected archive, and archives it in the system.
3. The archiver, at the end, logs a change audit record that the configuration of the device has changed, along with other Audit information.

4. If you have enabled the Enable Shadow Directory option in the Archive Settings dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt**) the latest running configuration file is also stored in a raw format for manual TFTP purposes to restore the configuration on the device, in the directory location:
   - On Solaris, /var/adm/CSCOpx/files/rme/dcma/shadow
   - On Windows, *NMSROOT*/files/rme/dcma/shadow. Where *NMSROOT* is the directory in which RME is installed (the default is C:\Program Files\CSCOpx)

Note Startup configurations are not 'versioned' and only one copy of the startup configuration of devices (which supports startup configuration), is saved in the system. No change audit records are logged for changes in the 'Startup Configuration' files.

RME first compares the collected configuration file, with the latest configuration in the archive, and checks to see if there are effective configurations changes from what was previously archived.

Change Audit Logging

Config change audit records include information about, who changed (which user) the configuration, when the configuration change was identified by RME, and other change information.

- Any configuration change made through the RME system (example, using Config Editor or Netconfig), will have the user name of the user who scheduled the change job.
- Any configuration change that was done outside of RME and detected through the configuration retrieval process, has the same user name as reported by the device through the *CONFIG-MAN-MIB* variable (ccmHistoryEventTerminalUser).
- Changes identified through syslog messages, contain the user name identified in the Syslog message, if present.

Defining the Configuration Collection Settings

The configuration archive can be updated with configuration changes in two ways:

- Periodic configuration archival (with and without configuration polling). You can enable this using **Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Collection Settings**.
- Manual configuration archival using **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive**.

You can modify how and when the configuration archive retrieves configurations by selecting one or all of the following:

Periodic Polling

The configuration archive performs a SNMP query on the device. If there are no configuration changes detected in the devices, no configuration is fetched.

Periodic Collection

The configuration is fetched without checking for any changes in the configuration.

By default, the Periodic Collection and Polling are disabled.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The following is the workflow for defining the configuration collection setting:

Step 1 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt** > **Collection Settings**.

The Config Collection Settings dialog box appears.

Step 2 Select one or all of the following options:

Periodic Polling

a. Select **Enable** for Configuration archive to performs a SNMP query on the device to retrieve configuration.

b. Click **Schedule**.

The Config Collection Schedule dialog box appears.

c. Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the configuration polling job. To do this, select one of these options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule.
Job Information	
Job Description	The system default job description, *Default config polling job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

d. Click **OK**.

Periodic Collection

a. Select **Enable** for Configuration archive to perform a periodic check on the device to retrieve configuration.

b. Click **Schedule**.

The Config Collection Schedule dialog box appears.

c. Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the configuration collection job. To do this, select one of these options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule.
Job Information	
Job Description	The system default job description, *Default config collection job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

d. Click **OK**.

Step 3 Either click **Apply to accept the new values provided**.

Or

Click **Cancel if you want to discard the changes and revert to previously saved values**.

If you had clicked Apply, a message appears:

```
New settings saved successfully.
```

You can check the status of your scheduled job by selecting **Resource Manager Essentials** > **Job Mgmt** > **RME Jobs**.

Purging Configurations from the Configuration Archive

You can specify when to purge archived configurations. This frees disk space and keeps your archive at a manageable size.

By default, the purging jobs are disabled.

You can purge configurations based on two criteria:

- Number of versions to retain. Maximum number of versions of each configuration to retain.

  The oldest configuration is purged when the maximum number is reached. For example, if you set the maximum versions to retain to 10, when the eleventh version of a configuration is archived, the earliest (first version) is purged to retain total number of latest archived versions at 10.

- Age. Configurations older than the number of days that you specify are purged.

  The Labeled configuration files are not purged even if they satisfy either of the purge conditions (Maximum versions to retain and Purge versions older than options in the Archive Purge Settings window) unless you enable the Purge labeled files option in the Archive Purge Settings window.

  The labeled files are purged only if they satisfy the conditions given in the Maximum versions to retain and Purge versions older than options.

Archive Management will not purge the configuration files, if there are only two versions of these files in the archive.

Archived configurations that match the purge criteria that you set are purged from the system. This purge policy applies to Running configuration only.

Caution Ensure that the configuration change detection schedule does not conflict with purging, since both processes are database-intensive. Also backup your system frequently to prevent losing versions.

Note View Permission Report (**Common Services** > **Server** > **Reports**) to check if you have the required privileges to perform this task.

The workflow to define the Configuration Archive purge policy is:

Step 1 Select **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt** > **Purge Settings**.

The Archive Purge Setup dialog box appears.

Step 2 Select **Enable**.

Step 3 Click **Change** to schedule a Purge job.

The Config Purge Job Schedule dialog box appears.

Step 4 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to purge the configuration archive files. To do this, select one of these options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule.
Job Information	
Job Description	The system default job description, *Default archive purge job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 5 Specify when to purge configuration files from the archive by selecting one or all of the following purge policies:

- Click **Maximum versions to retain** and enter the number of configurations to retain.
- Click **Purge versions older than** and enter the number of days, weeks, or months.
- Click **Purge labeled files** to delete the labeled configuration files. See Configuring Labels for information on labeled files.

  The Purge labeled files option must be used either with the Maximum versions to retain or Purge versions older than options. You cannot use this option without enabling either Maximum versions to retain or Purge versions older than options.

  The labeled files are purged only if they satisfy the conditions given in the Maximum versions to retain and Purge versions older than options.

  The Labeled configuration files are not deleted even if they satisfy either of the purge conditions (Maximum versions to retain and Purge versions older than) unless you enable the Purge labeled files option.

These purge policies are applied sequentially. That is, if you have enabled all the three purge policies, RME applies the Purge policies in this sequence:

a. Maximum versions to retain

b. Purge versions older than

c. Purge labeled files

Archive Management does not purge the configuration files, if there are only two versions of these files in the archive.

Step 6 Click **Apply**.

A message appears, `New settings saved successfully`.

Step 7 Click **OK**.

You can check the status of your scheduled job by selecting **Resource Manager Essentials** > **Job Mgmt** > **RME Jobs**.

Checking Configuration Archival Status

After you add devices into RME, their configurations are gathered and stored in the configuration archive. You can check the overall status of the configuration archive (Successful, Partially Successful, and Failed). It provides the status of the last archival attempt.

Refresh (Icon)	Click on this icon to refresh the configuration archive status window.

Note View Permission Report (**Common Services** > **Server** > **Reports**) to check if you have the required privileges to perform this task.

To check the configuration archive status:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt**.

The Configuration Archival Summary dialog window appears with the following information.

Archival Status	Description
Successful	Number of devices for which all supported configurations have been fetched successfully. Click **No.of Devices** to see the Successful Devices Report.

Archival Status	Description
Failed	Number of devices for which fetch of all supported configurations has failed. Click **No.of Devices** to see the Failed Devices Report.
Partial Successful	Number of devices for which fetch of any one of the supported configurations has failed. Number of Catalyst 5000 devices for which sub-modules were not pulled into archive. Only the main configuration of supervisor engine module is archived for Catalyst 5000 devices. Click **No.of Devices** to see the Partially Successful Devices Report.

Step 2 Select one or all of the Config Archival Status and click **Sync Archive** to schedule an immediate job to update the archive status.

You can check the status of your scheduled *Sync Archive* job by selecting **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

Configuration Archival Reports

The following are the Config Archival reports:

- Successful Devices Report
- Failed Devices Report
- Partially Successful Devices Report

Successful Devices Report

A device appears in this report if all supported configurations have been fetched successfully.

Note These dates do not necessarily reflect when the archive was last updated.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type that is either Running or Startup configuration.

Column Names	Description
Accessed At	Date and time that RME pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Displays the archival status.

Failed Devices Report

A device appears in this report if fetch for all of the supported configurations has failed. This report also contains the reasons configuration could not be pulled.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type that is either Running or Startup configuration.
Accessed At	Date and time that RME pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Reason why RME could not pull running and startup configuration from device.

If you enabled TACACS for a device and configured custom TACACS login and passwords prompts, you may experience Telnet problems, since RME may not recognize the prompts.

To make your prompts recognizable, you must edit the TacacsPrompts.ini file. See the procedure given in the Handling Custom Telnet Prompts section of the User Guide for Common Services.

Partially Successful Devices Report

A device shows up in this report if fetch for any one of the supported configurations has failed.

The Partially Successful Devices report lists the Catalyst 5000 family devices for which sub-module information could not be pulled from the device. Only the main configuration of the supervisory module is archived for Catalyst 5000 devices.

This report contains the following information:

Column Names	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
File Type	Defines the configuration file type that is either Running or Startup configuration.
Accessed At	Date and time that RME pulled running configuration from device in an attempt to archive. The configuration is archived only if there has been a change.
Description	Reason why RME could not pull running or startup configuration from device.

Scheduling Sync Archive Job

You can schedule a job to update the configuration archive for selected group of devices.

You have an option to poll device configuration before updating the archive and to fetch Startup configuration.

You can also perform this task for a selected device using Device Center (from the CiscoWorks LMS Portal home page, select **Device Troubleshooting > Device Center** to launch Device Center).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To schedule a job to update the device configuration:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Sync Archive**.

The Sync Archive dialog box appears.

Step 2 Select either:

- Device Selector, if you want to schedule a job for static set of devices. See Using RME Device Selector for information on how to use RME Device Selector.

Or

- Group Selector, if you want to schedule a job for dynamic group of devices.

  The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluates static groups also as dynamic during run time.

Step 3 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Sync Archive job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • 6 - hourly—Runs this task every 6 hours, starting from the specified time. • 12 - hourly—Runs this task every 12 hours, starting from the specified time. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	**Description**
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	
Poll device before configuration collection	Archive Management polls the device and compares the time of change currently on the device with the time of last archival of configuration to determine if configuration has changed on a device. If the polling is not supported on the device, then configuration fetch will be initiated without checking for the changes. See Understanding Configuration Retrieval and Archival for further details on configuration polling.
Fetch startup config	Archive Management fetches the startup configuration.

Step 4 Click **Submit**.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 5 Click **OK**.

You can check the status of your scheduled *Sync Archive* job by selecting **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

Generating an Out-of-Sync Report

You can generate an Out-of-Sync report for the group of devices for which running configurations are not synchronized with the startup configuration.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Out-of-Sync Summary** to generate an Out-of-sync report.

The Startup and Running Out-Of-Sync Summary window displays the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Startup	Startup configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to view the configuration.
Diff	Difference between the archived Startup and archived Running configuration. Click on the icon to see the difference between the archived Startup and archived Running configuration.
Running	Running configuration of the device. This configuration is fetched from the configuration archive. Click on the displayed date to see the detailed information on Running configuration.

Scheduling Sync on Device Job

You can schedule a Sync on device job using the Sync on Device button on Startup and Running Out-Of-Sync Summary window.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To schedule a Sync on device job:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Out-of-Sync Summary**.

The Startup and Running Out-Of-Sync Summary dialog box appears.

Step 2 Select a device.

Step 3 Click **Sync on Device**.

The Job Schedule and Options dialog box appears.

Step 4 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Startup and Running Out-Of-Sync Summary report. To do this, select one of these options from the drop-down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled Job Approval for Archive Management.
Maker E-Mail	Enter the e-mail-id of the job creator. This is a mandatory field. This field appears only if you have enabled Job Approval for Archive Management.
Job Options	
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 5 Click **Submit**.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 6 Click **OK**.

You can check the status of your scheduled *Copy Running Config to Startup* job by selecting **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

Using the Configuration Version Tree

You can view all configuration versions of the selected devices in the form of a graphical display. You can also perform a configuration quick deploy for a selected device.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To view the configuration Version Tree:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Version Tree**

The Device Selection dialog box appears.

Step 2 Select a device. See Using RME Device Selector for information on how to use RME Device Selector.

Step 3 Click **OK**.

The Config Version Tree dialog box appears.

Step 4 Click either the configuration version which is a hyper link or select the radio button for the configuration version.

To expand the configuration version folder, click on plus icon and select the configuration version to view the configuration.

The Config Viewer dialog box appears. See Understanding the Config Viewer Window for further information.

If you want to perform a configuration quick deploy (Configuration Quick Deploy), click the Deploy button.

Understanding the Config Viewer Window

The Config Viewer is a HTML-based window which displays the configurations of specified devices.

You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file.
- Click **Processed** to view data with the commands ordered and grouped.

The Config Viewer window contains two columns.

Column	Description
Configlets	Click on any configlets to display the corresponding information. The available configlets vary from device to device; the following are examples: • All—Entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, `snmp-server community public RO`. • IP Routing—IP routing configuration commands. For example, `router abcd 100`. • Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`. • Global—Global configuration commands. For example `no ip address`. • Line con 0—configuration commands for line console 0. • IP—IP configuration commands. For example, `ip http server`.
Configuration file name	View the contents of configuration file.

The buttons on the Config Viewer are:

Button	Description
Export (Icon)	Export the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory where Configuration Archive file is exported is: On RME Solaris server, /var/adm/CSCOpx/files/rme/dcma/configexport On RME Windows server, *NMSROOT*\files\rme\dcma\configexport
Export (continue)	To export a file: **1.** Click on the icon. The Export Config File dialog box appears. **2.** Enter the folder name on the RME server. You must enter the default export directory. You cannot enter any other directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html or Browse to select a folder on the RME server. The Server Side File Browser dialog box appears. **a.** Select a folder on the RME server. **b.** Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html **3.** Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*.`cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*.`XML` Where *ExportedFolder* is the location where configuration file is exported. **4.** Click **OK**.

Button	Description
Print (Icon)	Generates a format that can be printed.
Compare with previous version	Compares configuration with previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button gets activated only if you have a previous version of the configuration.
Compare with next version	Compares configuration with next version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button gets activated only if you have a next version of configuration.
Edit	Launches Config Editor window. This button is active only if you are viewing the configuration version from the archive. See Editing and Deploying Configurations Using Config Editor for further details.
Deploy	Perform a quick configuration deploy. This button is active only if you are viewing the configuration version from the archive. See Configuration Quick Deploy.

Viewing the Configuration Version Summary

You can view all archived configurations for selected devices. It also provides a link to view a particular configuration running on the device and to generate differences between versions in the archive.

You can view the last three configuration versions for each device regardless of number of versions stored in archive.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To view the Config Summary, follow this workflow:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Version Summary**

The Device Selection dialog box appears.

Step 2 Select a device. See Using RME Device Selector for information on how to use RME Device Selector.

Step 3 Click **OK**.

The Archive Mgmt Version Summary window appears with the information in Table 8-5.

Table 8-5 Fields in the Archive Mgmt Version Summary Window

Column	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Startup	Configuration running when device was started. This configuration is fetched from the device. Click on the Startup icon to view the Startup configuration
Diff	Differences between Startup and Running configuration. To view the difference between Startup and Running configuration, click on the Diff icon.
Running	Configuration currently running on device. Click on the Running icon to view the Running configuration. The configuration that appears, is fetched from the device. This happens if the fetched configuration is different from the latest configuration that is in the archive. Otherwise, the latest configuration from the archive appears.
Diff	Differences between the Running Configuration on the device and the most recent archived configuration. To view the difference between the two running configurations, click on the Diff icon.
Latest	Displays date and time of most recent configuration archive. The time shown here is when the file was actually archived. If the file was archived on 03/07/2004 5.00 PM PST, that's the time that will appear in this report. This is in the client's time zone. To view the device configuration, click on **Date** and **Time**. The Archived At fields that appear in other configuration reports shows the last time configuration was taken from the device in an attempt to archive. The system actually archives the configuration only if there is a change in the newly obtained configuration when compared to the archived one. So there could be different time values.
Diff	Differences between the most recent and the second most recent archived configurations. To view the difference between the two running configurations, click on Diff icon.
Latest-1	Date and time the second most recent configuration was archived. To view the device configuration, click on date and time.
Diff	Differences between second most recent and third most recent configuration in archive. To view the difference between the two running configurations, click on the Diff icon.
Latest-2	Date and time third most recent configuration was archived. To view the device configuration, click on **Date** and **Time**.

Configuration Quick Deploy

You can create an immediate job to deploy the version of configuration being viewed on the device. You can deploy the configuration either in overwrite or merge mode.

Features of Configuration Quick Deploy

The following are the features of Configuration Quick Deploy:

- It can be performed for both running and startup configuration of all categories of devices.
- The job is executed immediately. Therefore Job approval should not be enabled at the time of Configuration Quick Deploy.
- The jobs cannot be rolled back.
- The jobs use TFTP, Telnet, SSH, scp, rcp, https transport protocols.
- It provides an option to select either merge or overwrite mode when you deploy configuration on a device.
- It cannot be performed for VLAN configurations. However, you can deploy VLAN configurations using the CLI command, `cwcli config put`. See Overview: cwcli config Command for more information.
- It is supported for configuration versions in the archive only. That is, you cannot deploy for configuration version available on a device.
- The jobs use the same protocol order that you have specified in the Config Transport Settings (**Resource Manager Essentials** > **Admin** > **Config Mgmt**).

Performing a Configuration Quick Deploy

You can perform a configuration quick deploy using the Config Viewer window.

For example, you can launch Config Viewer window by clicking on Startup configuration or Running Configuration links while performing tasks such as generating Out-Of-Sync Summary report, viewing the Version Summary report etc.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Click **Deploy** on the Config Viewer (Understanding the Config Viewer Window) window.

The Job Option Details dialog box appears.

Step 2 Enter the following information:

Field	Description
Job Information	
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.
Deploy Mode	
Overwrite	Select the **Overwrite** option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (RME assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.
Merge	Select the **Merge** option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.

Step 3 Click **Submit**.

An immediate Quick Deploy of Configuration on Device job will be scheduled.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 4 Click **OK**.

You can check the status of your scheduled *Config Quick Deploy* job by selecting **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

What Happens During Configuration Quick Deploy

Before Configuration Management deploys the configuration on the device, it verifies whether the device is locked.

The deploy process follows the configured transport protocol order and the fallback option is active.

At end of this task, Configuration Management will:

- Unlock the device
- Checks-in the new version of configuration if the deploy completes successfully.

After uploading the configuration on the device, Configuration Management writes to the Change Audit log.

Configuring Labels

A label is a name given to a group of customized selection of configuration files. You can select configuration files from different RME devices, group and label them.

These labeled files are not purged along with the other configuration files. You have to explicitly select the Purge labeled files option to purge the labeled files. These labeled files are not purged if this option is not enabled.

You can purge the label config files using **Resource Manager Essentials** > **Admin** > **Config Mgmt** > **Archive Mgmt** > **Purge Settings.**

See Purging Configurations from the Configuration Archive for further details.

The Label Config window displays the following information:

Column	Description
Label Name	Displays the label name.
Description	Displays the label description.
Created by	Displays the user who created this label.
Created on	Displays the label creation time.

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.

The Label Configs window contains the following buttons:

Button	Description
Create	Create a label. See Creating a Label for further details.
Edit	Edit a labeled configuration. See Editing a Labeled Configuration for further details. This button is active only after you select a Label.
View	View a labeled configuration. See Viewing the Labeled Configuration for further details. This button is activate only after you select a Label.
Delete	Delete labeled configuration. See Deleting the Labeled Configuration for further details. This button is activate only after you select a Label.

Creating a Label

You can use Label Configuration to create a group of configuration files from selected devices.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You can create a label file using the following workflow:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Label Configs**.

The Label Configs dialog box appears.

Step 2 Click **Create**.

The Device Selection dialog box appears.

Step 3 In Device Selector pane, select the devices. See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Go to the Label selection pane and:

- Enter the Label Name. You can enter up to 64 characters.
- Enter the Label Description. You can enter up to 128 characters.

Step 5 Go to the Config Type pane and select **Primary** or **VLAN**.

Option	Description
Primary	Contains the Running and Startup configuration files information.
VLAN	Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information.

Step 6 Go to the Version pane and select **Latest** to include the most recent configuration only, or **All** to view all configuration versions.

- If you have selected Latest, you can click **Finish** button in the Select Devices page and complete the Label creation.
- If you have selected All, go to Step 7.

Step 7 Click **Next**.

The Select Configs to be Labelled dialog box appears.

- To view the configuration, select a configuration version file from the left pane and click **View**. The Config Viewer (Understanding the Config Viewer Window) window appears.
- To add the selected configuration, select a configuration version file from the left pane and click **Add**.
- To remove the selected configuration, select a configuration version file from the right pane and click **Remove**.

Step 8 Click **Finish**.

A message appears, `Label` *LabelName* `created successfully`.

Where *LabelName* is the name of the label that you entered.

Step 9 Click **OK**.

Editing a Labeled Configuration

You can make the following changes to a label:

- Modify the Label Description.
- Remove configuration files from the Selected Versions list.
- Add new configuration files from the Devices list.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You can edit a label file using the following workflow:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Label Configs**.

The Label Configs dialog box appears.

Step 2 Select a label and click **Edit**.

The Device Selection dialog box appears. The devices that are already part of the labeled file are selected.

Step 3 Go to the Device Selector pane and select a new device or deselect a device. See Using RME Device Selector for information on how to use RME Device Selector

Step 4 Go to the Version pane and select **Latest** to include the most recent configuration only, or **All** to view all configuration versions.

Step 5 Click **Next**.

The Label Details dialog box appears. This dialog box appears with the current details of the label.

Step 6 Do either of the following:

- Change the Label Description. You can enter up to 128 characters.
- Select a configuration version file from the left pane, click **Add** to add the selected configuration file.
  - If you selected **Latest** in the previous dialog box, the left pane will show devices and the latest archived configuration file. The right pane contains labeled configuration.
  - If you selected **All** in the previous dialog box, the left pane will show devices and all available archived configuration files. The right pane contains labeled configuration.

Note You can select only one configuration file for a device.

- To remove the selected configuration, select a configuration version file from the right pane and click **Remove**.
- To view the configuration, select a configuration version file from the left pane and click **View**. The Config Viewer (Understanding the Config Viewer Window) window appears.

Step 7 Click **Finish**.

A message appears, `Label` *LabelName* `updated`.

Where *LabelName* is the name of the label as entered by you.

Step 8 Click **OK**.

Viewing the Labeled Configuration

You can view configurations of a label from the label listing.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Label Configs**.

The Label Configs dialog box appears.

Step 2 Select a label and click **View**.

The Label Config Viewer window appears with the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.

Column Name	Description
Version	Version of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file. In the Config Viewer window, you can click the Deploy button if you want to perform a Configuration Quick Deploy (Configuration Quick Deploy)
Created On	Date and time configuration file was created.
Change Description	Description of configuration change.

Deleting the Labeled Configuration

You can delete a label from the list of labels in the label configuration dialog box:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Label Configs**.

The Label Configs dialog box appears.

Step 2 Select the labels and click **Delete**.

A message appears, `Are you sure you want to delete the label(s)?`

Step 3 Click **OK** to delete the labels.

Using Search Archive

You can search the archive for configuration containing text patterns for selected devices. You can specify ten different combinations of patterns/strings as part of search criteria.

For example:

- Search all devices for configurations having pattern **`set banner motd`** and **`set banner exec`**.
- Search all devices for configurations having pattern **`set banner motd`** and **`set banner exec`** and **`set password`**.

You can also specify an option to ignore/consider the case sensitive property.

You can create a custom configuration query that searches information about the specified configuration files.

If you monitor devices X, Y, and Z every morning, you can create a custom query on them. When you run the query, RME quickly gathers all the archived configuration files for these devices and displays them in a report.

The Custom Queries window displays the following information:

Column	Description
Query Name	Custom Query name.
Description	Custom Query description.
Created By	User name of the person who created this Custom Query.
Created On	Custom Query creation time.

You can click on any column heading to sort the information by that column. If you double-click a heading, the order is reversed.

The Custom Queries window contains the following buttons:

Button	Description
Create	Create a custom query. See Creating a Custom Query for further details.
Edit	Edit a custom query. See Editing a Custom Query for further details. This button is activate only after you select a custom query.
Run	Run a custom query. See Running a Custom Query for further details. This button is activate only after you select a custom query.
Delete	Delete custom queries. See Deleting the Custom Queries for further details. This button is activate only after you select a custom query.

The user who creates the custom query has the full permission to perform any tasks such as edit, run, etc,. on the Custom Queries.

See Searching Archive for the procedure to search the configuration with and without search pattern.

Creating a Custom Query

To create a custom query:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive > Custom Queries**.

The Custom Queries dialog box appears

Step 2 Click **Create**.

Step 3 Do any of the following:

- Enter the Custom Query name. You can enter up to 64 characters.
- Enter the Custom Query description. You can enter up to 128 characters.
- Enter patterns to search for, for example, *http server*. You can enter text patterns up to 64 characters.

To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria.

You cannot search for special characters or regular expressions, for example, *Control-C*, *boot**, etc.

- Select the search criteria **Contains/Does Not Contain**.
- If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings.
- Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.

Step 4 Click **OK**.

A message appears, `Custom Query` *CustomQueryName* `created successfully`.

Where *CustomQueryName* is the name of the custom query as entered by you.

Step 5 Click **OK**.

Running a Custom Query

To run a custom query:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Search Archive** > **Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Run**.

The Device Selection dialog box appears.

Step 3 Select the devices. See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Click **OK**.

The Custom Query Search Result window appears with the following information:

Column Name	**Description**
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Version	Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file. In the Config Viewer window, you can click on the Deploy button if you want to perform a configuration quick deploy (Configuration Quick Deploy)
Created On	Date and time configuration file was created.

You can perform the following tasks from this window:

- Select the devices and click **NetConfig** to make any changes to the device configuration using NetConfig templates.
- Select a device and click **Edit** to edit the device configuration using the Config Editor application.

Editing a Custom Query

You can edit the Custom Query description and modify the search patterns and their criteria. To edit a custom query:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive > Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Edit**.

The Custom Query Window appears.

Step 3 Do any of the following:

- Update the Custom Query description. You can enter up to 128 characters.
- Either add a new search pattern or delete or update an existing search pattern and their criteria. You can enter up to 64 characters.
- Modify the string search options Match Any to Match All or vice versa.
- Enable/Disable the case-sensitive search.

Step 4 Click **OK**.

A message appears, `Custom Query` *CustomQueryName* `updated successfully`.

Where *CustomQueryName* is the name of the Custom Query.

Step 5 Click **OK**.

Deleting the Custom Queries

To delete the custom queries:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt Archive Mgmt Search Archive Custom Queries**.

The Custom Queries dialog box appears.

Step 2 Select a Custom Query and click **Delete**.

A message appears, `The query will be deleted`.

Step 3 Click **OK**.

Searching Archive

You can search the device configuration file with or without the search pattern. You can also narrow down your search using Label Configuration files and Custom Queries.

You can view the search report in two ways:

- Search Archive Result
- Device Configuration Quick View Report

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To search the configuration archive:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Search Archive**.

The Search Archive dialog box appears.

Step 2 Enter the following:

Field	Description
Left Pane	
Label Config	Enable this option and select a label name. The configuration version options Latest and All are disabled.
Device Selector	Select the devices. See Using RME Device Selector for information on how to use RME Device Selector. If you have selected Label Config, you need not select devices. If you have selected any devices, only the devices that are specified in the label configuration are searched. Other devices are ignored.

Field	Description
Version	Select **Latest** to search the most recent configuration only or **All** to search all configuration versions. If you have selected Label Config, then you cannot specify the versions.
View Type	Select one of these view types: • **Version** to view the Device Configuration Version Report. This displays all versions of the configuration, the time and date the configurations were archived, and reason for archival. • Click **Quick View** to view the Device Configuration Quick View Report. This displays the contents of the configuration files.
Right Pane	
Custom Query	Select a Custom Query. The search patterns that are defined in the Custom Query appear in the Pattern Details text boxes. In addition to Custom Query search patterns, you can also add additional search patterns.
Pattern Details	Perform the following tasks: • Enter patterns to search for, for example, *http server*. You can enter text patterns up to 64 characters. To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria. You cannot search for special characters, for example, *Control-C, boot**, etc. You can search the device configuration file without the search pattern too. The search will list all archived configuration for all selected devices. – If you have selected the version as **Latest,** the search will list latest archived configuration for all selected devices. – If you have selected the version as **All,** the search will list all archived configurations for all selected devices • Select the search criteria **Contains/Does Not Contain**. • If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings • Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.

Step 3 Click **Search**.

Based on your View type selection, either Search Archive Result or Device Configuration Quick View Report appears.

Search Archive Result

The Search Archive Result displays information about the device configurations. The Search Archive Result contains the following details of the selected configurations:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This config type does not contain Startup configuration file information. For ONS devices, the PRIMARY config type displays the configuration information from the active CPU, at that instance.
Version	Versions of configuration file. Click on the version to display Config Viewer (see Understanding the Config Viewer Window), which shows contents of corresponding configuration file.
Created On	Date and time configuration file was created.
Change Description	Cause of configuration change.

You can perform the following tasks from this window:

- Select the devices and click **NetConfig** to make changes to the device configuration using NetConfig templates.
- Select a device and click **Edit** to edit the device configuration using the Config Editor application.

Device Configuration Quick View Report

The Device Configuration Quick View report lists the devices, configuration version numbers, and configuration details of the device configuration version you specified.

You can specify how you want to view the contents of the configurations by selecting one of the options under Show:

- Click **Raw** to view data exactly as it appears in the configuration file. There are two panes, one lists all devices and the other displays the configuration.
- Click **Processed** to view data with the commands ordered and grouped. There are three panes, one lists all devices, the second pane lists all configlets, and the third pane displays the configuration.

Column	Description
Devices	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
Configlets	You can click on any configlets to display the corresponding information. The available configlets vary from device to device. The following are examples: • All—The entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, **`snmp-server community public RO`**. • IP Routing—IP routing configuration commands. For example, **`router abcd 100`**. • Interface folder—The different interface configuration commands. For example, **`Interface Ethernet0`** and **`Interface TokenRing`**. • Global—Global configuration commands. For example **`no ip address`**. • Line con 0—Configuration commands for line console 0. • IP—IP configuration commands. For example, **`ip http server`**.
Configuration file name	You can view the contents of configuration file.

The following buttons are available on the Config Viewer:

Button	Description
Export (Icon)	Exports the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory where Configuration Archive file is exported is: On RME Solaris server, /var/adm/CSCOpx/files/rme/dcma/configexport On RME Windows server, *NMSROOT*\files\rme\dcma\configexport

Button	**Description**
Export (continue)	To export a file: **1.** Click on the icon. The Export Config File dialog box appears. **2.** Enter the folder name on the RME server. You must enter the default export directory. You cannot enter any other directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html or Browse to select a folder on the RME server. The Server Side File Browser dialog box appears. **a.** Select a folder on the RME server. **b.** Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html **3.** Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.XML` Where *ExportedFolder* is the location where configuration file is exported. **4.** Click **OK**.
Print (Icon)	Generates a format that can be printed.
Compare with previous version	Compares configuration with the previous version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button is activate only if you have a previous version of configuration.
Compare with next version	Compares configuration with the next version. When you click on this button, a new window Config Diff Viewer opens to show configurations side by side. See Understanding the Config Diff Viewer Window for further details. This button is activate only if you have a next version of configuration.

Button	**Description**
Edit	Launches Config Editor window. This button is active only if you are viewing the configuration version from the archive. See Editing and Deploying Configurations Using Config Editor for further details.
Deploy	You can perform a configuration quick deploy. This button is active only if you are viewing the configuration version from the archive. See Configuration Quick Deploy.

Comparing Configuration

You can compare two device configuration files from version to version or from device to device. You can also compare the configuration when a device was started with the current configuration, and the current configuration with the most recently archived configuration.

You can list the commands that have to be excluded while comparing configurations.

To do this select **Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Exclude Commands**. See Configuring Exclude Commands for further details.

You can compare the configurations in these ways:

- Startup vs. Running—Compares the configuration when the device was started with the current configuration. These configurations are fetched from the device.

  See Comparing Startup vs. Running Configurations.
- Running vs. Latest Archived—Compares the running configuration with the most recent archived configuration. The Running configuration is fetched from the device.

  See Comparing Running vs. Latest Archived Configurations.
- Two Versions of the Same Device—Compares two archived configuration versions.

  See Comparing Two Configuration Versions of the Same Device.
- Two Versions of Different Devices—Compares any two configurations in the configuration archive.

  See Compare Two Configuration Versions of Different Devices.

Comparing Startup vs. Running Configurations

You can compare the configuration when a device was started with the current configuration. These configurations are fetched from the device.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To compare Startup vs. Running configurations:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Startup vs. Running** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Click **OK**.

The Understanding the Config Diff Viewer Window window appears.

Comparing Running vs. Latest Archived Configurations

You can compare the configuration currently running on a device with the most recent configuration stored in the configuration archive. The Running configuration is fetched from the device.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To compare Running vs. latest archived configurations:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Running vs. Latest Archived** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Click **OK**.

The Understanding the Config Diff Viewer Window window appears.

Comparing Two Configuration Versions of the Same Device

You can compare two different archived configurations of the same device.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To compare two versions of the same device:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Two Versions of the Same Device** and click **Compare**.

The Device Selection dialog box appears.

Step 3 Select a device. See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Click **Next**.

The Select First Configuration dialog box appears with the following information:

Column Name	Description
Config Version	Versions of configuration file.
File Type	Defines the configuration file type that is either Running or Startup configuration.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Created On	Date and time configuration file was created.

Step 5 Click on the first configuration to compare and click **Next**.

The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

Step 6 Click on the second configuration to compare it with first configuration and click **Finish**.

The Understanding the Config Diff Viewer Window window appears.

Compare Two Configuration Versions of Different Devices

You can compare two archived versions of a configuration of the same or different devices.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To compare two versions of different devices:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Compare Configs**.

The Compare Configurations dialog box appears.

Step 2 Select **Two Versions of Different Devices** and click **Compare**.

The Select Device and Pattern dialog box appears.

Step 3 Perform the following and click **Next**:

Field	Description
Left Pane	
Device Selector	Select the devices. See Using RME Device Selector for information on how to use RME Device Selector.
Version	Select **Latest** to view the most recent configuration or **All** to view all configuration versions.
Right Pane	
Pattern Details	Perform the following tasks: 1. Enter patterns to search for, for example, *http server*. You can enter text patterns up to 64 characters. To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields. You can specify ten different combinations of patterns as part of search criteria. You cannot search for special characters or regular expressions, for example, *Control-C, boot**, etc. You can search the device configuration file without the search pattern too. 2. Select the search criteria **Contains/Does Not Contain**. If you have entered string as a search pattern, you can select **Match Any** to search for any given pattern string or **Match All** to search for all pattern strings. 3. Click **Match Case** to perform a case-sensitive search, which is more efficient when you know the exact pattern you want to match. By default, Match Case is disabled.

The Select First Configuration dialog box appears with the following information:

Column Name	Description
Device Name	Device Display Name as entered in Device and Credential Repository.
Config Version	Versions of configuration file.
File Type	Defines the configuration file type that is either Running or Startup configuration.
Config Type	Defines the type of configuration PRIMARY, SECONDARY, or VLAN. • PRIMARY/SECONDARY—Contains the Running and Startup configuration files information. • VLAN—Contains running vlan.dat configuration file information. This configuration type does not contain Startup configuration file information. For ONS devices, the PRIMARY configuration type displays the configuration information from the active CPU, at that instance.
Created On	Date and time configuration file was created.

Step 4 Click on the first configuration to compare and click **Next**.

The Select Second Configuration dialog box appears with the same information as the Select First Configuration window.

Step 5 Click on the second configuration to compare it with first configuration and click **Finish**.

The Understanding the Config Diff Viewer Window window appears.

Understanding the Config Diff Viewer Window

The Configuration Version Compare report shows the differences between the two selected configurations. You can access the Configuration Version Compare report by comparing device configurations.

You can specify how you want to view the differences between the configurations by selecting one of the options under Show:

- Click **Raw** to view the differences between the two raw configurations.
- Click **Processed** to view the differences with the commands ordered and grouped.

The color conventions that are used on Config Diff Viewer are:

- Black—All unchanged text.
- Red—Lines that have changed from one version to another.
- Blue—Lines that have been added or deleted from one of the versions.

The Configuration Versions Compare report has three columns:

Column	Description
Configlets	You can click on any configlet to display the corresponding information. The available configlets vary from device to device. The following are examples: • Diffs—Displays the differences between the two configuration files (if you selected more than one). • All—The entire contents of the configuration files. • SNMP—SNMP configuration commands. For example, `snmp-server community public RO`. • IP Routing—IP routing configuration commands. For example, `router abcd 100`. • Interface folder—The different interface configuration commands. For example, `Interface Ethernet0` and `Interface TokenRing`. • Global—Displays global configuration commands. For example `no ip address`. • Line con 0—Displays configuration commands for line console 0. • IP—Displays IP configuration commands. For example, `ip http server`.
First configuration file	Contains the contents of the first configuration file.
Second configuration file	Contains the contents of the second configuration file.

The buttons on the Config Diff Viewer are:

Button	Description
Export (Icon)	Export the configuration file. • If you are using the Raw mode then the exported file format is cfg. The file name convention is *DeviceName-VersionNumber*.cfg. • If you are using the Processed mode then the exported file format is XML. The file name convention is *DeviceName-VersionNumber*.xml. Where *DeviceName* is the device Display Name as entered in Device and Credential Repository and *VersionNumber* is the device configuration version. The default directory where Configuration Archive file is exported is: On RME Solaris server, /var/adm/CSCOpx/files/rme/dcma/configexport On RME Windows server, *NMSROOT*\files\rme\dcma\configexport

Button	Description
Export (continue)	To export a file: **1.** Click on the icon. The Export Config File dialog box appears. **2.** Enter the folder name on the RME server. You must enter the default export directory. You cannot enter any other directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html or Browse to select a folder on the RME server. The Server Side File Browser dialog box appears. **a.** Select a folder on the RME server. **b.** Click **OK**. The Browse button takes you to the default directory. It does not allow you to change this default export directory. To change the default directory, see the RME 4.x FAQs section: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_troubleshooting_guide09186a008036dff2.html **3.** Click **OK**. If you have exported configuration in the Raw mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.cfg` If you have exported configuration in the Processed mode, the notification message displays, `Config file exported as` *ExportedFolder\DeviceName-VersionNumber*`.XML` Where *ExportedFolder* is the location where configuration file is exported. **4.** Click **OK**.
Print (Icon)	Generates a format that can be printed.

Using Archive Management Job Browser

You can browse the Archive Management jobs that are registered on the system. From the Archive Mgmt Jobs dialog box you can also retry, delete, stop jobs and view a job's details.

The Archive Management Jobs window displays the following information:

Column Name	**Description**
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the Job ID to view the Archive Management Job Details (see Viewing the Archive Management Job Details).
Job Type	Type of the configuration job. • Sync Archive—Appears if you had scheduled a Sync Archive job (Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive). • Get Config—Appears if you had scheduled a configuration fetch job using the CLI command, **`cwcli config get`**. • Put Config—Appears if you had scheduled a configuration retrieve job using the CLI command, **`cwcli config put`**. • Import Config—Appears if you had scheduled a job that retrieved the configuration from a file and if you had transferred it to the device using the CLI command, **`cwcli config import`**. • Write to Running Config—Appears if you had scheduled a job that downloaded the differences between the specified configuration file and the latest configuration version in the archive for the specified device, using the CLI command, **`cwcli config write2run`**.
Job Type (Continue)	• Write to Startup Config—Appears if you had scheduled a job that erased the contents of the device Startup configuration and if wrote contents of a specified file as new Startup configuration, using the CLI command, **`cwcli config write2start.`** • Copy Running Config to Startup—Appears if you had scheduled a job that overwrote with the Startup configuration of the device with the Running configuration, using the CLI command, **`cwcli config run2start`**. • Copy Startup Config to Running—Appears if you had scheduled a job that merged the Startup configuration with the Running configuration, using the CLI command, **`cwcli config start2run`**. • Reload Device—Appears if you had scheduled a job that rebooted the devices, using the CLI command **`cwcli config reload`**. • Config Quick Deploy—Appears if you had created an immediate Configuration Quick Deploy job, using the Config Viewer window. • Compliance Check—Appears if you had scheduled a Compliance Check job (Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance and clicked the Compliance Check button). • Deploy Compliance Results—Appears if you had scheduled a Deploy job on the non-complaint devices (Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance and clicked the Deploy button). • Check Compliance and Deploy—Appears if you had scheduled a Compliance Check job with the job option, Check compliance and deploy enabled (Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance and clicked the Compliance Check button). • Deploy Baseline template—Appears if you had scheduled a Baseline Template deploy job (Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates and clicked the Deploy button).

Column Name	Description
Status	Job states: - Cancelled—Running job stopped by you. - Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. This count of failed devices is not displayed for jobs restored from RME 4.0.4 or lesser versions. - Running—Job still running. - Scheduled—Job scheduled to run. - Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details. - Successful—Job completed successfully - Waiting for Approval—Job waiting for approval.
Description	Job description entered during job definition
Owner	User who created this job.
Scheduled at	Date and time job is scheduled to run.
Completed at	Date and time at which job completed.
Schedule Type	Run type of the job: Immediate, Once, 6 - hourly, 12 - hourly, Daily, Weekly, and Monthly.

You can click on any column heading to sort information by that column. If you double-click on a heading, the order is reversed.

You can use the Filter button to do a quick search on the Archive Management jobs. You can perform filters by using these options:

Filter Options	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Job Type	Types of Archive Management jobs. For example: Sync Archive, Write to Running Config, etc.
Status	Status of the job. For example: Successful, Failed, etc.
Description	Job description.
Owner	Owner of the job.
Schedule Type	Job schedule Type. For example: Immediate, Weekly, etc.

Refresh (Icon)	Click on this icon to refresh the Archive Management Job Browser.

You can perform the following tasks on this window:

- Retrying a Config Job
- Stopping a Config Job
- Deleting the Config Jobs
- Viewing the Archive Management Job Details
- Scheduling Sync Archive Job
- Generating an Out-of-Sync Report
- Scheduling Sync on Device Job
- Baseline Template

Retrying a Config Job

You can retry only a failed job. You cannot retry a job that are scheduled to run periodically (Daily, Weekly, and Monthly).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To retry a job:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

The Archive Management Jobs dialog box appears.

Step 2 Select a failed job and click **Retry**.

The Job Schedule and Options dialog box appears.

Step 3 Enter the following information:

Based on your retry job selection, some of the options may not be visible.

For example, 6 - hourly and 12 -hourly Run Type options are visible only if you are retrying a Sync Archive job. This is not visible for other types of Archive Management jobs.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the selected retry job. To do this, select one of these options from the drop-down menu: • 6 - hourly—Runs this task every 6 hours, starting from the specified time. • 12 - hourly—Runs this task every 12 hours, starting from the specified time. • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Information	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Archive Management.
Maker E-Mail	Enter the e-mail-id of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Archive Management.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 4 Click **Submit**.

A message appears, `Job resubmitted successfully`.

Step 5 Click **OK**.

Stopping a Config Job

You can stop the following running job types (See Using Archive Management Job Browser for details on the job types):

- Put Config
- Import Config
- Write to Running Config
- Write to Startup Config
- Copy Running Config to Startup
- Copy Startup Config to Running
- Reload Device

- Config Quick Deploy
- Check Compliance and Deploy
- Deploy Baseline template
- Compliance check

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To stop a Archive Management job:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

The Archive Management Jobs dialog box appears.

Step 2 Select a running job and click **Stop**.

A message appears, `Selected job(s) will be stopped`.

Step 3 Click **OK**.

Deleting the Config Jobs

You can delete the job in these status:

- Cancelled
- Failed
- Scheduled
- Rejected
- Successful
- Waiting for Approval

You cannot delete a running job.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To delete jobs:

Step 1 Select **Resource Manager Essentials** > **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

The Archive Management Jobs dialog box appears.

Step 2 Select a running job and click **Delete**.

A message appears, `Selected job(s) will be deleted`.

Step 3 Click **OK**.

Viewing the Archive Management Job Details

From the Archive Management Jobs window, you can learn more about one job by viewing its details. You can view this details by clicking the Job ID on the Config Job window.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The Archive Management Job Details window contains the following information:

Page/Folder	Description
Execution Summary	Displays summary of completed job: • Execution Summary—Information about the job status, start time and end time. • Device Summary—Information about the job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully. Click on Device Details folder and device status link and on the Device link to see the complete job execution details. • Execution Message (Pre-Execution and Post-Execution)—Information about any e-mails sent.
Device Details	Contains detailed job results for each device. Displays status folders that correspond to possible device status: • Successful Devices—Devices were successfully executed. • Failed Devices—Devices were not successfully executed. • Partially Failed Devices—Job partially failed to run on these devices. • Pending Devices—Job did not try to update devices, even though they were selected. • Not Attempted—Job did not attempt to run on these devices. Click on **Status** to see the job details. Details include a record of the entire CLI session between RME and the device. To launch the Device Center, click on the device display name. When the configuration fetch takes unusually long, this error message appears, `Unable to get results of job execution for device. Please retry the job` This could happen because of slow device response, Network latency, etc.
Work Order	Contains the Summary of the job definition such as, • Detailed information, such as owner, schedule type, and Job Approval state. • Policies configured for the job, such as E-mail Notification and Job Based Password. • Devices on which the job runs. Also, gives details about the commands. For retried jobs, these job definitions are not updated. For such jobs the original job definitions are retained.

The buttons on the Job Details window are:

- Delete—You can delete jobs with the following Job Status:

  - Cancelled
  - Failed
  - Scheduled
  - Rejected
  - Successful
  - Waiting for Approval

You cannot delete a running job.

- Stop—You can stop the following running job types (See Using Archive Management Job Browser for details on the job types):
  - Put Config
  - Import Config
  - Write to Running Config
  - Write to Startup Config
  - Copy Running Config to Startup
  - Copy Startup Config to Running
  - Reload Device
  - Config Quick Deploy
  - Check Compliance and Deploy
  - Deploy Baseline template
  - Compliance check

Baseline Template

You can identify a set of standardized policy based commands that you would want to have on a set of devices.

You can create a Baseline template which is a set of commands identified through the process of baselining, which contain placeholders for device-specific values to be substituted.

For example:

`set vtp domain` [*name*] **`password`** [*xxx*]

`set snmp community read-write` [*Read write community string*]

When you add a new device of the same type to the network, you can use the existing Baseline template, which consists of two parts, command and values. You can create configurations for any device of the same type to the network by specifying the values for the variables in the baseline template.

The following section contains:

- Features of Baseline Template
- Defining Commandsets

Features of Baseline Template

The features of Baseline Template are:

- You can use this Baseline template to compare with other device configuration and generate a report that lists all the devices which are non-compliant to the Baseline template.
- You can easily deploy the Baseline template to the same category of devices in the network.
- You can schedule a compliance check job and deploy the Baseline template onto the non-compliant devices. This can be performed as a single job or as a separate job.
- You can import or export a Baseline template. This template is stored in XML format.

The rules for specifying the Baseline templates are:

- All the commands that are disallowed should begin with a "-".
- All commands that are mandatory should begin with a "+".
- Commands that do not begin with (- or +) are considered as comments and ignored.
- The command values can be a wildcard match.

  `+ ip address` [*ip-address*] [*netmask*]

  `+ ip address` [**`#10\.76\.38\..*#`**] [*netmask*]

  `+ ip address` [**`#10\.72\..*\..*#`**] [*netmask*]

  To find a match for any octet in an IP address you must use **`\..*`**.

  In the examples shown above, the command will apply for all the devices with the IP address starting with 10.76.38.* [netmask] and 10.72.*.* [netmask].
- The regular expressions must be enclosed with **`#`**.

  For example:

  `snmp-server location` [#.*#]

  This command will fail compliance check for snmp-server location loc1 loc2 loc3, because the check will be performed only for one word after snmp-server location.

  To overcome this, you have to define the command as:

  + [# **`snmp-server location`** .*#]

  Then the compliance check will be performed for all forms of snmp-server commands like snmp-server location loc1 loc2.....n,etc.
- Negation in Regular expressions :

Use Case 1:When there are more than one entry in the Config files.
Commands in Device Config :

logging name1

logging name2

logging name3

Template: **`+logging [#!name1#]`**

Details : The negation of the name1 is done which returns true, since there are other logging commands present with other names. So the template is compliant.

Use Case 2: When there is only one entry in the Config files.

Commands in Device Config :

logging name1

Template: **`+logging [#!name1#]`**

Details : The negation of the name1 is done which returns False. Since there is no other command with logging statement except "logging name1" , the template is Non-Compliant.

Use Case 3**:** When there is no logging commands

Commands in Device config :

No logging commands

Template :`+ logging [# !name1 #]`

Details: First the negation of the name1 is done which returns False. Since there are no login commands, the template is Non-compliant.

- The Baseline template uses java.util.regex engine for regular expressions. For more information, see the regex API guide for Java 1.4.2 from Sun:

  http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html
- Submode commands are provided only if the commands are to be compared inside a submode.

  For example:

  interface [#*Ethernet*.*#]

  `+ no shutdown`

  `no shutdown` command will apply to all interfaces with *Ethernet*.

Defining Commandsets

The commandsets are a set of one or more CLI commands. You can define a commandset while creating a Baseline template in the Advanced mode.

The features of the commandsets are:

- If the commands in commandset are in a submode (ip/interface etc.) a submode command must be specified for such a commandset.
- Commandsets can have one or more child commandsets.
- Child commandsets inherit parent’s sub-mode command.

You can define commandsets that have to be checked before running the actual commands.

The features of the prerequisite commandsets are:

- A commandset can have another commandset as its prerequisite.
- A prerequisite commandset is used only for comparison and is not deployed onto the device.
- A commandset is compared with the config only if its prerequisite condition is satisfied.

The RME evaluates the commandsets in different ways depending on whether you have defined the commandset as Parent or Prerequisite.

For example assume that you have defined two commandsets, commandset1 and commandset2:

- Commandset defined as Prerequisite

  commandset1 as the Prerequisite of commandset2. While RME evaluates the Baseline template, commandset1 is evaluated first and commandset2 is evaluated next.

  If commandset1 does not contain submode and is not present in a device, then commandset2 is not evaluated and the device is displayed in excluded list in compliance report.

  If commandset1 contains submode and is not present in applicable submodes , then commandset2 is not evaluated and the device is displayed in excluded list in compliance report.
- Commandset defined as Parent

commandset1 as the Parent of commandset2. While RME evaluates the Baseline template, commandset1 is evaluated first and commandset2 is evaluated next.

If either of these commandsets is missing, the template is considered non-compliant.

Baseline Templates Window

This window lists all the user-defined Baseline templates. It also displays the following details of the Baseline template:

Column Name	Description
Name	Name of the Baseline template.
Device Type	Type of the device for which the defined Baseline template can be used.
Description	Description of the Baseline template. If you have imported Baseline templates, the description given is *Imported baseline*.
Created On	Displays the Baseline template creation date and time.

You can click on any column (except Baseline Name) to sort the information by that column. If you double-click a heading, the order is reversed.

This window contains the following buttons:

Button	Description
Create	Create a Baseline template. See Creating a Baseline Template for further details.
Edit	Edit a Baseline template. This button is activate only after you select a Baseline Name. See Editing a Baseline Template for further details
Export	Export a Baseline template file. This button is activate only after you select a Baseline Name. See Exporting a Baseline Template for further details.
Import	Import a Baseline template file. See Importing a Baseline Template for further details.
Delete	Delete a Baseline template. This button is activate only after you select a Baseline Name. See Deleting a Baseline Template for further details.

Button	Description
Deploy	Deploy a Baseline template. This button is activate only after you select a Baseline Name. See Deploying a Baseline Template for further details.
Compliance Check	Perform compliance check with Baseline template. This button is activate only after you select a Baseline Name. See Running Compliance Check for further details.

Creating a Baseline Template

You can create a Baseline Template by:

- Creating a Basic Baseline Template
- Creating an Advanced Baseline Template

There are few example templates which are available. You can use these templates as a base to create new templates.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Creating a Basic Baseline Template

To create a Basic Baseline template:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates window appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 In the Template Details section, select **Basic** as the mode.

Step 4 Enter the following information:

Field	Description
Name	Name of the Baseline template. You can enter only alphanumeric characters (including spaces) up to 254 characters. Do not enter any special characters. This includes underscores and hyphens.
Description	Description for the Baseline template. You can enter up to 254 characters.
Device Type Selector	Device family for which you can apply this template. Click the check box to select the device family.

Step 5 Click **Next**.

Step 6 The Add Template Details dialog box appears.

Enter the CLI command under the Baseline Template.

CLI Commands	This is a mandatory field. Enter the CLI commands. For example: **`Routers CLI Commands`** **`+ set snmp community read-write`** [*read-write-community-name-string*] **`- set snmp community read-only public`** **Explanation:** • The first line is considered as a comments since it does not begin with either "+" or "-". • The second line is mandatory since it begins with "+". • The third line is disallowed since it begins with "-". In the above example, *read-write-community-name-string* is a command value. The command value should not contain spaces.

A message appears, `Successfully created the template` *BaselineTemplateName*.

Where *BaselineTemplateName* is the Template Name as given by you.

Step 7 Click **OK**.

The Baseline Templates window appears with the newly created Baseline template.

Creating an Advanced Baseline Template

To create an Advanced Baseline template:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The select Creation Mode dialog box appears.

Step 3 Select **Advance** as the mode from the Template Details section.

Step 4 Enter the following information:

Field	Description
Name	Name of the Baseline template. You can enter only alphanumeric characters (including spaces) up to 254 characters. Do not enter any special characters. This includes underscores and hyphens.
Description	Description for the Baseline template. You can enter up to 254 characters.
Device Type Selector	Device family for which you can apply this template. Check the check box to select the device family.

Step 5 Click **Next**.

The Add Template Details dialog box appears.

Step 6 Enter the following information:

Field	**Description**
Commandset Options	
Name	Name of the commandset. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.
Parent	Enter the parent name for the commandset, if required. This is case sensitive. You can also use this to logically group the commandsets. For example: To work on ATM permanent virtual connections (PVCs) commands, you must first get into the interface mode from the global mode and then run the PVC specific-commands. Commandset 1: ATM **`interface`** *[#atm.*#]* **`+ ip address`** *[ip-addr] [net-mask]* Commandset 2: PVC *[#pvc.*#]* **`+ encapsulation aal5`** *[encap-type]* **`+ abr`** *[output-pcr1] [output-mcr]* **`+ ubr`** *[output-pcr2]* **`+ vbr-nrt`** *[output-pcr3] [output-scr] [output-mbs]* **`+ vbr-rt`** *[peak-rate] [average-rate] [burst]* **`+ protocol ip`** *[proto-ip] [type]* **`+ exit`** Here, commandset 1 is the parent for commandset 2. While RME evaluates the Baseline template, commandset1 is evaluated first and commandset2 is evaluated next. If either of these commandsets is missing, the template is considered non-compliant.

Field	Description
Prerequisite	Select the mandatory commandset name that you must enter before running the current commandset. In the example (See Mark as Prerequisite row), if you had marked commandset 1 as the Prerequisite, you can select *commandset 1: IntCheck* from the drop-down menu. Before running the commandset 2, the commandset 1 is run. That is, commandset1 is evaluated first and commandset2 is evaluated next. If there is no commandset1, commandset2 is not evaluated and the template is considered compliant.
Mark as Prerequisite	1. Select the checkbox to mark a particular commandset as a prerequisite. For example, Commandset 1: IntCheck **`interface`** *[intname]* **`+ ip address`** *[#10\.76\.38\..*#] [net-mask]* (To find a match for any octet in an IP address you must use **`\..*`**.) 2. Select the Mark as Prerequisite check box for the *Commandset 1: IntCheck*. For example, Commandset 2: IntDownload **`interface`** *[intname]* **`+ no cdp enable`** 3. Select the Prerequisite from the dropdown menu for the *Commandset 2: IntDownload*. If a commandset has a Prerequisite commandset, you cannot select the Mark as Prerequisite check box for that particular commandset. That is, in the above example, you cannot select the checkbox Mark as Prerequisite for *Commandset 2:IntDownload*.

Field	Description
CLI Commands	
Submode	Enter the command to get into interface mode from the global mode. For example: **`interface`** [*intname*] Here, **`interface`** is a command keyword and *intname* is command value. The command value should not contain spaces. You can also run the command for a set of interfaces. For example: **`interface`** [#*Ethernet.**#] Here, the command will be executed on all the interfaces having Ethernet.
Ordered Set	Select this option to make the system consider the order of the commands while performing compliance check. In other words, the commands in the device config should appear in the same order as that of the CLI commands definition order in the Command Set.
CLI Commands	Enter the CLI commands. For example: **`# Routers CLI Commands`** **`+ set snmp community read-write`** [*read-write-community-name-string*] **`- set snmp community read-only public`** **Explanation:** • The first line is considered as a comment since it begins with a “#”. • The second line is mandatory as it begins with “+”. • The third line is disallowed as it begins with “-”. There should be a space between the commands and the “-” or “+”. If there is no space, the commands are considered as comments and ignored. In the above example, *read-write-community-name-string* is a command value. The command value should not contain spaces.

- If you want to add a new commandset to the template click **Add**. The CLI Commands window is displayed with the default help comments. These help comments serve as guidelines to create commandsets.
- If you want to delete a Commandset from the Command set list, click **Delete**.
- If you want to preview the changes to the Commandset details before finishing up the creation of the template, click **Preview**. The changed Commandset details is displayed in a window.
- If you click **Save**, for the first time, a message appears,
  `Do you wish to create a new template?.`
- If you click **Save**, for the second time, a message appears,
  `Successfully updated the template` *BaselineTemplateName*.

  If the Commandsets consist of Prerequisite commandset then these commandsets appear in red color in the Preview details.
- If you want to reset the changes made to a Commandset, click **Reset**

Step 7 Click **OK**.

A message appears,

`Successfully created the template` *BaselineTemplateName*.

Where *BaselineTemplateName* is the name of the Baseline Template.

Step 8 Click **OK**.

If you want to add one more commandset repeat this procedure from Step 4.

Step 9 Click **Finish**.

A message appears,

```
Do you wish to save the changes?.
```

Step 10 Click **OK**.

A message appears,

```
Successfully created the template.
```

Step 11 Click **OK**.

The Baseline Configs window appears with all the available Baseline templates.

Creating an Advanced Baseline Template— Example

Example 1

This is a procedure to create a Baseline template to disable CDP on an interface that belongs to a specific subnet.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 Select **Advanced** and click **Next**.

The Create a Baseline dialog box appears.

Step 4 Enter the following information:

Field	User data
Template Name	DisablingCDP You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters except underscores.
Device Type	Routers
Description	Baseline Template for DisablingCDP
Commandset Option	
Name	PrerequisiteCheck. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.

Field	User data
Parent	Global
Prerequisite	Do not select any value.
Mark as Prerequisite	Select the check box to mark the commandset as prerequisite.
CLI Commands	
Submode	interface [*intname*] Where, *intname* is a variable. The variables should not contain spaces.
Ordered Set	Select this so that the system considers ordering of commands while performing compliance check.
CLI Commands	**`+ ip address`** _[#10\.76\.38\...*#] [netmask]_ To find a match for any octet in an IP address you must use **`\..*`**. This checks for subnet mask with IP address starting from 10.76.38.*.

Step 5 Click **Save**.

A confirmation message appears that the template will be created.

Step 6 Click **OK**.

A confirmation message appears that the template is created.

Step 7 Click **OK**.

To add another commandset within the same Baseline template, Disabling-CDP, enter the following information.

Field	User data
Commandset Option	
Name	DisableCDP. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.
Parent	Global
Prerequisite	Select the PrerequisiteCheck from the dropdown menu.
Mark as Prerequisite	Do not select the checkbox.
CLI Commands	
Submode	interface [*intname*]
Ordered Set	Select this so that the system considers ordering of commands while performing compliance check.
CLI Commands	**`+ no cdp enable`** This will disable the CDP in all the interfaces even if any one interface contains the subnet mask starting with IP address 10.76.38.*.

Step 8 Click **Save**.

A confirmation message appears that the template is updated.

Step 9 Click **OK**.

Step 10 Click **Finish**.

A confirmation message appears that the template will be saved.

Step 11 Click **OK**.

A confirmation message appears that the template is updated.

Step 12 Click **OK**.

The Baseline Configs window appears with the details of Disabling-CDP Baseline template.

Example 2

This is a procedure to create an Advanced Baseline Template to check the presence of the command "ip address 10.77.209.8 255.255.255.224" in the Ethernet interfaces which has cdp disabled.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Click **Create**.

The Select Creation Mode dialog box appears.

Step 3 Select **Advanced** and click **Next**.

The Create a Baseline dialog box appears.

Step 4 Enter the following information:

Field	User data
Template Name	CheckIPTemplate You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters except underscores.
Device Type	Routers
Description	Baseline Template for Interface level check.

Field	User data
Commandset Option	
Name	PrerequisiteCheck. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.
Parent	Do not enter anything.
Prerequisite	Do not select any value.
Mark as Prerequisite	Select the check box to mark the commandset as prerequisite.
CLI Commands	
Submode	interface [#Ethernet.*#]
Ordered Set	Do not select the checkbox.
CLI Commands	`+ no cdp enable`

Step 5 Click **Save**.

A confirmation message appears that the template will be created.

Step 6 Click **OK**.

A confirmation message appears that the template is created.

Step 7 Click **OK**.

To add another commandset within the same Baseline template, CheckIPTemplate, enter the following information.

Field	User data
Commandset Option	
Name	IPCheck. You can enter only alphanumeric characters up to 254 characters. Do not enter any special characters. This includes spaces, underscores and hyphens.
Parent	PrerequisiteCheck
Submode	Do not enter anything
Prerequisite	Select the PrerequisiteCheck from the dropdown menu.
Mark as Prerequisite	Do not select the checkbox.
CLI Commands	
Submode	Do not enter anything
Ordered Set	Do not select the checkbox.
CLI Commands	`+ ipaddress` *10.77.209.8 255.255.255.224* The above command will be deployed in the Ethernet interfaces which have the CDP disabled.

Step 8 Click **Save**.

A confirmation message appears that the template is updated.

Step 9 Click **OK**.

Step 10 Click **Finish**.

A confirmation message appears that the template will be saved.

Step 11 Click **OK**.

A confirmation message appears that the template is updated.

Step 12 Click **OK**.

The Baseline Configs window appears with the details of CheckIPTemplate Baseline template.

Editing a Baseline Template

You can edit all the Baseline template fields except for Template Name.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To edit the Baseline templates:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template.

Step 3 Click **Edit**.

The Select Creation Mode dialog box appears. The mode that you have selected while creating the Baseline template is retained. You cannot change this mode.

- You can provide a description in the Description text field.
- You can select or deselect devices in the Device Type Selector listbox.

Step 4 Click **Next.**

The Add Template Details dialog box appears.

Step 5 Select the commandset which you want to edit.

Step 6 Edit the required information.

See Creating an Advanced Baseline Template for more information on field descriptions for the fields that appear in the Add Template Details dialog box.

Step 7 Click **Finish**.

A message appears, `Template is modified. Do you wish to save the changes?`

Step 8 Click **OK**.

A notification appears, `Successfully updated the template` *BaselineTemplateName*.

Step 9 Click **OK** to save changes.

Exporting a Baseline Template

You can export a Baseline template. The exported file is in XML format.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To export a Baseline Template:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select one or many Baseline templates and click **Export**.

The Export a Baseline Template dialog box appears.

Step 3 Either:

- Enter the folder name. The file will be exported on the RME server.

or

a. Click **Browse**.

The Server Side File Browser dialog box appears.

b. Select a folder.

c. Click **OK**.

Step 4 Click **OK**.

A message appears, `Template exported as` *User_Specificed_Directory**Template Name*`.xml`

The naming convention followed for the baseline parameter file is *Template Name*.xml.

The file will be exported on the RME server at the specified path.

Importing a Baseline Template

To import a Baseline Template:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Import**.

The Import a Baseline Template dialog box appears.

Step 3 Enter the name of the Template file.

The file will be imported.

or

a. Click **Browse**.

The Server Side File Browser dialog box appears.

b. Select the XML file.

c. Click **OK**.

Step 4 Click **OK**.

A message appears, `Template successfully imported`.

Step 5 Click **OK**.

The imported file appears in the Baseline Templates window with the description, Imported baseline.

Deleting a Baseline Template

To delete a baseline template:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select one or more Baseline templates and click **Delete**.

A message appears, `The selected Template will be permanently deleted`.

Step 3 Click **OK**.

A message appears, `Successfully deleted the template`.

Step 4 Click **OK**.

The selected Baseline Template is removed from the Baseline Templates window

Note You can delete Example Templates.

Deploying a Baseline Template

When you add a new device of the same type to the network, you can use the existing Baseline template. This template consists of two parts, command and values.

You can create configurations for any device of the same type to the network by specifying the values for the variables in the Baseline template.

You can deploy Baseline template on the RME devices in two ways:

- User Interface (See Deploying a Baseline Template Using User Interface for the procedure.)

- File System (See Deploying a Baseline Template Using File System for the procedure.)

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Deploying a Baseline Template Using User Interface

To deploy a Baseline template using User Interface:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Deploy**.

The Deploy Input Options dialog box appears.

Step 3 Select **Enter Data From User Interface** and click **Next**.

The Select Devices dialog box appears.

The device list contains only that particular Device Type devices that you have selected while creating the Baseline Template.

For example, if you have selected Device Type as Router, only routers are listed.

Step 4 Select devices under the following tabs:

- In the All tab,

  Devices are grouped under All Applicable Devices and All Applicable Device Groups. All Applicable Device Groups categories devices under Routers, Switches, and so on.

- In the Search Results tab,

  The results of simple search and advanced search are listed here. For details on Search, see Using RME Device Selector, page 3-68

- In the Selection tab,

  All the devices that are selected are listed and you can deselect the devices.

Step 5 Click **Next**.

The Commands Generation dialog box appears.

Step 6 Perform the following tasks:

Field Name	Description and Action
Device list	This pane lists the selected devices that you have selected in the Select Devices dialog box. Select the device for which you want to deploy the Baseline template.
Edit	Select a device from the device drop down list and click on Edit button to edit information for the device.
Save	Click **Save** to save the changes made for the selected device. You can change the details for multiple devices in one go, by using the Save button.
Device	The selected device in the Device List pane is displayed in this text box.

Field Name	Description and Action
Commandsets	The pane contains all the commandsets that are defined in the Baseline template. Select a commandset. While creating the Baseline template, if you have defined the multiple occurrences as the commandset feature, after selecting that particular commandset, the *Add Instance* button is activated.
Add Instance	This button is activate only if you have selected a commandset with multiple occurrences. The occurrences of a commandset are defined while creating the Baseline template. When you click on the Add Instance button, one more instance of multiple commandset is added in the Commandsets pane. Enter the command value for that commandset in the Device Data pane.
Delete Instance	Use the Delete Instance button to delete the instance after selecting the instance from the Commanlets pane. You can select one or more instances and click on the Delete Instance button to delete the instances. You can delete the selected instances. The exception being that atleast one instance of the commandlet is available.
Templates	The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.
Device Data	The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: **`Interface`** [*#Ethernet[.*]#*] **`+ no shutdown`** Then, *#Ethernet[.*]#* is the command value. The Device Data field names appear as: `#Ethernet.*`[*0*] If the commandset is a prerequisite commandset, you do not need to specify parameter values for the Device data field as they are not deployed.

Step 7 Click **Next**.

The Job Schedule dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template deploy job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Archive Management.
Maker E-Mail	Enter the e-mail-id of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Archive Management.

Field	**Description**
Copy Running Config to Startup	Select to cause job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 9 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 10 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

Step 11 Click **OK**.

You can check the status of your scheduled job using **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**. The Job Type for this deploy job is Deploy Baseline template result.

Deploying a Baseline Template Using File System

You can deploy a Baseline template using the Baseline Parameter file.

You can generate this parameter file using **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > View** (button).

See Exporting a Baseline Template for further information.

To deploy a Baseline template using File System:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Step 2 Select a Baseline template and click **Deploy**.

The Deploy Input Options dialog box appears.

Step 3 Select **Enter Data From File System** and click **Next**.

The Select Input File dialog box appears.

Step 4 Enter the folder name and the file name with the file format extension XML.

or

a. Click **Browse**.

The Server Side File Browser dialog box appears.

b. Select the XML file.

c. Click **OK**.

The Select Input File dialog box appears with the selected Baseline Parameter file.

Step 5 Click **Next**.

The Job Schedule dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template deploy job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Archive Management.
Maker E-Mail	Enter the e-mail-id of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Archive Management.
Copy Running Config to Startup	Select to make the job to write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 7 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 8 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

If you have specified incorrect filename/XML file format or if the hostname field is not updated, an error message appears, `Specified file could not be read. Please specify a valid file name.`

See Exporting a Baseline Template for further information.

Check the XML file format or update the hostname field and restart this procedure from Step 2.

Step 9 Click **OK**.

You can check the status of your scheduled job using **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**. The Job Type for this deploy job is Deploy Baseline template result.

Using Baseline Jobs

You can check the status of the Baseline jobs using **Config Mgmt > Archive Mgmt > Baseline Templates > Baseline Jobs.**

This window contains the following information:

Field Name	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.
Description	Job description entered during job definition.
Compliant/Deployed Device(s)	Displays how many devices are complaint out of total number of devices that were selected while creating the compliance job. Click on the link to view the Baseline Compliance Report (see Understanding the Baseline Compliance Report).
Status	Status of the job. The displayed job states are Successful, Failed, and Running. The jobs may have failed either because: • The device configuration is not archived. Or • The device is not reachable. The further details of the failed job is given in the **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs** (see Using Archive Management Job Browser). You can also check the status of the Baseline job at **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs** (see Using Archive Management Job Browser).

The Compliance Jobs window contains the following buttons:

Buttons	Description
Deploy	You can schedule a job to deploy the standard configuration to all non-compliance devices. This button is activate only after selecting a Compliance Jobs. See Deploying the Commands.
Delete	You can delete the compliance jobs. This button is activate only after selecting a Compliance Jobs. See Deleting the Compliance Jobs

Refresh (Icon)	Click on this icon to refresh the Compliance Jobs Window.

Running Compliance Check

To execute a compliance check:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates**.

The Baseline Templates dialog box appears.

Select the template and click **Compliance Check**.

The Select Devices dialog box appears.

Step 2 Select either:

- Device Selector, if you want to schedule a job for static set of devices. See Using RME Device Selector for information on how to use RME Device Selector.

Or

- Group Selector, if you want to schedule a job for dynamic group of devices.

  The job is scheduled only for the devices that are present in the selected group at the time when the job is run. The customizable group selector for jobs evaluate static groups also as dynamic during run time.

Step 3 Click **Next**.

The Schedule dialog box appears.

Step 4 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Baseline template compliance job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Field	Description
Job Options	
Check compliance and deploy	Enable this to check the compliance of the archived file with that of the Baseline template and deploy the commands if it non-compliant.
Copy Running Config to Startup	This option is active only if you select the Check compliance and deploy option. Select to make the job to write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Step 5 Click **Next**.

The Job Work Order window appears with the job details that you have selected.

Step 6 Click **Finish**.

A message appears, `Job` *JobID* `is created successfully`.

Where *JobID* is a unique Job number.

Step 7 Click **OK**.

You can check the status of your scheduled job by selecting **Config Mgmt > Archive Mgmt > Baseline Template > Compliance** or **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**.

Understanding the Baseline Compliance Report

The Baseline Compliance Report contains the following information:

Field Name	Description
Summary	
Template Name	Name of the Baseline template entered at the time of creating the Baseline template.
Number of Non-Compliant device(s)	Number of devices that are non-compliant.
Number of Compliant device(s)	Number of devices that are compliant.

Field Name	Description
Number of Excluded device(s):	List of devices where the job did not run. The jobs may have failed either because: • The device configuration was not archived. Or • The device was not reachable. The further details of the failed job is given in the Config Mgmt > Archive Mgmt > Archive Mgmt Jobs (See Using Archive Management Job Browser).
Compliant Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Latest Version	Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of corresponding configuration file against which the compliance was checked.
Created On	Date and time configuration file was created.
Non-Compliant Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Latest Version	Version of configuration file against which the compliance was checked. Click on the version to display Config Viewer (see Understanding the Config Viewer Window). This shows the contents of corresponding configuration file against which the compliance was checked.
Created On	Date and time configuration file was created.
Command(s) to Deploy	List the commands where the device configuration is non-compliant.
Excluded Devices	
Device Name	Device Display Name as entered in Device and Credential Repository.
Reason for Exclusion	Displays the cause for exclusion.

In addition, this report contains two buttons:

Button	Description
Export to File (Icon)	Exports this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Deploying the Commands

You can deploy the commands on the devices that are non-complaint.

Before you use this Deploy button, you must run the Compliance Report,

- If there are any non-complaint device, you must select the relevant compliance job and deploy the baseline template.

- If there are no non-complaint device and if you click on the Deploy button, a message appears,

  ```
  Could not deploy selected Job.
  Reason: No Non-Compliant devices present in the report.
  ```

  Click on the Job ID to view the Baseline Compliance Report. See Understanding the Baseline Compliance Report for further details.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To deploy the commands:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance**.

The Compliance Jobs dialog box appears.

Step 2 Select a Compliance Job.

Step 3 Click **Deploy**.

The Substitute Parameters for Devices dialog box appears.

Step 4 Perform the following:

Field Name	Description and Action
Device list	The list contains all the devices which are non-complaint. Select a device.
Device	The selected device in the Device List pane appears in this text box.
Commandsets	The pane contains all the commandsets that are defined in the Baseline template. In the Baseline template, if you have defined the multiple occurrences as the commandset feature then based on the compliance check, the commandset will appear more than once. Select a commandset.
Templates	The pane contains the CLI commands for the selected commandset. You cannot modify the commands in this pane.
Device Data	The field displays the command values that you have defined in your Baseline template. The command value is appended with a unique number. Enter the command value. For example: If your Baseline template contains this command: **`+ ip address`** [_#10\.76\.38\..*#_] [_netmask_] Then, _#10\.76\.38\..*#_ and _netmask_ are the command values. The Device Data field names appear as: _#10\.76\.38\..*#_[1000] _netmask_[1000]

If you have more than one device to deploy then you have to repeat Step 4 for all the devices.

Step 5 Click **Next**.

The Job Schedule dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the deploy configuration job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time.
Date	You can select the date and time (hours and minutes) to schedule. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	
Approver Comments	Enter comments for the job approver. This field appears only if you have enabled job approval for Archive Management.
Maker E-Mail	Enter the e-mail-id of the job creator. This is a mandatory field. This field appears only if you have enabled job approval for Archive Management.
Copy Running Config to Startup	Select to make the job to write the Running configuration to the Startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password Or – disable the Job Password option in the Job Schedule and Options dialog box.

Step 7 Click **Next**.

The Work Order dialog box appears with job details that you have entered.

Step 8 Click Finish.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 9 Click **OK**.

You can check the status of your scheduled job using **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs**. The Job Type for this deploy job is Deploy Baseline comparison result.

Deleting the Compliance Jobs

You can delete the job that have been completed or stopped. You cannot delete a running job.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To delete Compliance jobs:

Step 1 Select **Resource Manager Essentials > Config Mgmt > Archive Mgmt > Baseline Templates > Compliance**.

The Compliance Jobs dialog box appears.

Step 2 Select a job and click **Delete**.

A message appears, `The selected job will be deleted`.

Step 3 Click **OK**.

The selected Compliance job is removed from the Compliance Jobs window.

You can also delete the compliance jobs from **Config Mgmt** > **Archive Mgmt** > **Archive Mgmt Jobs** window (see Using Archive Management Job Browser)

CHAPTER 9

Making and Deploying Configuration Changes Using NetConfig

NetConfig allows you to make configuration changes to your network devices, whose configurations are archived in the Configuration Archive. NetConfig is a part of RME Configuration Management applications.

It provides easy access to the configuration files for all RME supported devices.

NetConfig automatically updates the Configuration Archive when it makes device configuration changes.

NetConfig provides many advantages over configuring devices from the CLI. For example, you can:

- Schedule jobs for future execution. You can schedule periodic jobs.
- Use configuration tasks to make configuration changes more easily and reliably.
- Run multiple commands during a job.
- Run commands on multiple devices during a job.
- Use the Job Approval application to require approval before a job can run.
- Roll back configuration changes made to devices when a job fails.

NetConfig Tasks

As a NetConfig user, you can:

- Define and schedule NetConfig jobs:

  To make configuration changes to managed devices, you define and schedule NetConfig jobs using the job definition wizard. You can use configuration tasks (system-defined or user-defined) to create the configuration commands that you want to apply to devices.

- Browse and edit NetConfig jobs:

  You can browse all NetConfig jobs on your system and edit, copy, stop, retry or delete them. For more information about a particular job, you can click the job details by clicking on the hyperlink of the Job ID in the NetConfig Job Browser.

- Use the command line interface for NetConfig jobs:

  You can use the cwcli command line interface to create and schedule NetConfig jobs from the command line.

As a NetConfig administrator, you can:

- Create User-defined tasks:

  You can create your own user-defined tasks containing any configuration or rollback commands, and download them to a set of selected devices. You enter the configuration commands by typing them or by importing them from a file.

  User-defined tasks can be parameterized. That is, they can contain variables that take values from a specified file that resides on the RME server.

- Assign tasks:

  As a network administrator, you can assign access to execute tasks, to CiscoWorks users with network operator privilege. You can assign one or more task, to one or more users. By default, only network administrators (users with Network Administrator permissions) can use configuration tasks.

- Separate protocol ordering for configuration deploy and fetch operations

  You can separately specify the protocol order for configuration download and update operations, for NetConfig jobs. This feature enables you to use your preferred protocols for downloading and fetching configuration.

  For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of NetConfig.

- Set the default NetConfig job policies

Each NetConfig job has job properties (including enabling job password) that define how the job will execute. You can configure defaults for these properties that will be applied to all future jobs. You can specify for each property whether users can change the default when creating a job.

See Understanding NetConfig User Permissions.

For the new features in this release, see What's New in this Release.

Note You can select the log level settings for the NetConfig application using the feature Application Log Level Settings (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

Preparing to Use NetConfig

- Verifying Device Credentials.
- Verifying Device Credentials
- Modifying Device Security
- Verifying Device Prompts
- Configuring Default Job Policies
- Assigning Task Access Privileges to Users
- Enabling Job Approval

Verifying Device Credentials

To verify that every device you want to configure has correct credentials in Device and Credential Repository, use the Device Credential Verification option (**Resource Manager Essentials > Devices > Device Management > Device Credential Verification**).

For more details see the topic Checking and Viewing Device Credentials in the section Adding and Troubleshooting Devices Using Device Management.

NetConfig must have access to the credentials to make device configuration changes.

Modifying Device Security

NetConfig must be able to run certain commands on devices to configure them. You must disable security that prohibits NetConfig from running these commands.

For the list of commands, see the topic Modifying Device Security in the section Archiving Configurations and Managing Them Using Archive Management.

Verifying Device Prompts

NetConfig requires particular CLI prompt formats:

If the telnet transport mechanism is used, the following prompts are applicable.

- For IOS-based devices, Content Engine devices, and Content Service Switch devices:
  - The login prompt must end with a greater-than symbol (>).
  - The enable prompt must end with a pound sign (#).
- For Catalyst devices:
  - The login prompt must end with a greater-than symbol (>).
  - The enable prompt must end with the text (enable).

If the secure shell (SSH) transport mechanism is used, the following prompts are applicable.

- For IOS-based devices, Content Engine devices, and Content Service Switch devices:
  - The login prompt may end with any one of the following: (>), (#), (:), (%).
  - The enable prompt must end with a pound sign (#).
  - For Catalyst devices:
  - The login prompt may end with any one of the following: (>), (#), (:), (%).
  - The enable prompt must end with the text (enable).

Default prompts use this formatting. If you have changed your defaults, verify that the prompts meet these requirements, and change them if they do not.

Configuring Default Job Policies

NetConfig jobs have properties that determine how they run. You can configure default job policies (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies)** that apply to all NetConfig jobs.

For more details see the topic Configuring Default Job Policies in the section Archiving Configurations and Managing Them Using Archive Management.

Assigning Task Access Privileges to Users

You can assign task access privileges that determine which configuration tasks each user can use to create NetConfig jobs. See Understanding NetConfig User Permissions.

Enabling Job Approval

You can enable Job Approval, (**Resource Manager Essentials > Admin > Approval > Approval Policies)** which means all jobs require approval before they can run.

For more details see the topic Setting Up Job Approval in the section Enabling Approval and Approving Jobs Using Job Approval.

Rolling Back Configuration Changes

NetConfig lets you roll back (undo) the configuration changes made to network devices if a job does not complete. How rollback commands (the configuration commands that are used to roll back the configuration changes) are created depends on how the job was created.

You must configure a NetConfig job to automatically roll back configuration changes if the job fails to complete.

NetConfig can rollback configuration only devices whose configurations are archived in the Configuration Archive. For details see Archiving Configurations and Managing Them Using Archive Management.

To verify that devices have an archived configuration and troubleshoot those that do not, use the Configuration Archival Summary dialog box (**Resource Manager Essentials > Config Mgmt > Archive Mgmt**). For more details see the topic Checking Configuration Archival Status in the section Archiving Configurations and Managing Them Using Archive Management.

Creating Rollback Commands

You can create rollback commands for a job in the following ways:

- If you use a system-defined task, rollback commands are created automatically by the task.
- If you create a user-defined task, you can enter rollback commands into the task.

Configuring a Job to Roll Back on Failure

You can define a job failure policy so it automatically rolls back configuration changes if the job fails to run. You can select one of several rollback options:

- Rollback device and stop—Rolls back the changes on the failed device and stops the job.
- Rollback device and continue—Rolls back the changes on the failed device and continues the job.
- Rollback job on failure—Rolls back the changes on all devices and stops the job.

Understanding NetConfig User Permissions

Access to NetConfig functionality is controlled by permissions.

Users with only Help Desk permissions cannot use NetConfig as this option will not be displayed for these users. Other users can use NetConfig, but their access to functionality is controlled by permissions.

In your application, see the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform the required NetConfig task.

Job Approval Permissions

Only users with Approver permissions can approve NetConfig jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

For more details see the topic Setting Up Job Approval in the section Enabling Approval and Approving Jobs Using Job Approval.

User-defined Tasks Permissions

By default, only users with Network Administrator permissions can create user-defined configuration tasks (see Creating and Editing User-defined Tasks).A network administrator must give other users permission to use them on a per-task basis.

Administrator Task Permissions

Only users with Network Administrator permissions can perform administrator tasks, which are listed in the NetConfig Admin menu. Other users will not see this menu.

Administrator tasks are:

- Assigning tasks to users.
- Configuring default job properties.
- Creating and editing user-defined tasks.

For user permissions, see Understanding NetConfig User Permissions.

Job Editing Permissions

After a NetConfig job is created, the owner, another user with the owner’s privileges, or a network administrator can:

- Copy a job.
- Edit a job
- Retry a job
- Delete a job
- Stop a job while it is running.

Using the NetConfig Tab

The NetConfig tab of RME enables you to do the following tasks:

- Create or edit NetConfig jobs, using the NetConfig job browser. You can also copy, retry, stop or delete jobs. You can run a job immediately. You can also schedule a job to run at a specified time, once, or periodically. See:
  - Starting a New NetConfig Job
  - Browsing and Editing Jobs Using the NetConfig Job Browser
- Create your own NetConfig tasks and run them on a selected set of devices. See Creating and Editing User-defined Tasks.
- Assign tasks to users. You can assign one or more tasks, to one or more users. See Assigning Tasks to Users.

Starting a New NetConfig Job

Use the job definition wizard to create and schedule a NetConfig job.

To browse and edit jobs using the NetConfig job browser, see Browsing and Editing Jobs Using the NetConfig Job Browser.

Ensure that you have set the:

- Transport protocol order for your job using **Resource Manager Essentials > Admin > Config Mgmt**.

  For more details see the topic Configuring Transport Protocols in the section Archiving Configurations and Managing Them Using Archive Management.
- Job and password policy for your job using **Resource Manager Essentials > Admin > Config Mgmt >Config Job Policies** before starting a new NetConfig job.

  For more details see the topic Configuring Default Job Policies in the section Archiving Configurations and Managing Them Using Archive Management.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To start a new NetConfig job:

Step 1 Select **Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs**.

The NetConfig Job Browser appears.

For the fields in the NetConfig Job Browser, see Browsing and Editing Jobs Using the NetConfig Job Browser.

Step 2 Click **Create**.

The Devices and Tasks dialog box appears, with these panes:

Pane	Description
Device Selector	Allows you to select the devices on which the NetConfig job has to run. You can select multiple device categories. Only in the case of cable devices, you should select only one device for which to create a job.
Task Selector	Allows you to select the system-defined tasks or user-defined tasks that you want to run on the selected devices. For descriptions of system-defined tasks and the device categories they support, see Using System-defined Tasks. For creating and using User-defined tasks, see Creating and Editing User-defined Tasks.

Step 3 Select the devices from the Device Selector pane.

See the topic Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management.

Step 4 Select the required task from the All tab, using the Task Selector.

You can select one or more task at a time. Your selection appears in the Selection pane.

Step 5 Click **Next.**

The Add Tasks dialog box appears with these panes:

Pane	Description
Applicable Tasks	Allows you to add a task. The task that you selected using the Task Selector, appears here. From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. If the task that you have selected does not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane. Select a task and click **Add** to create an instance for the task (see Step 6).
Added Instances	Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task, and click the required button (see Table 9-1).

Table 9-1 Tasks Performed by Buttons in the Added Instances Pane

Button	Description
Edit	Task pop-up opens with previously assigned values. You can modify these values and click **Save**.
View CLI	Device Commands pop-up opens with the list of applicable devices and their corresponding CLI commands. Devices in your selection for which the commands are not applicable, are also displayed as Non-Applicable Devices. Click **Close** to close the pop-up window. You can modify an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.
Delete	Deletes the selected task instance. You can delete an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.

Step 6 Select an applicable task from the Applicable Tasks pane and click **Add**.

The Task (system-defined or user-defined) pop-up appears for the selected task.

Step 7 Set the parameters in the task dialog box and click **Save**.

(To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.)

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format:

Taskname_n, where *Taskname* is the name of the task you have added, and *n* is the number of the instance. For example, the first instance of a Banner task is `Banner_1`.

You can add as many instances as required, for a task.

Step 8 Click **Next**.

The Job Schedule and Options dialog box appears with these panes:

Pane	**Description**
Scheduling	Allows you to schedule the job.
Job Options	Allows you to set the job options.

Step 9 Set the schedule for the job, in the Scheduling pane:

Field	**Description**
Scheduling	
Run Type	Select the run type or frequency for the job—Immediate, Once, Daily, Weekly, Monthly, or Last Day of Month. If Job Approval is enabled, the Immediate option is not available.
Date	Select the start date for the job.
at	Select the start time for the job from the hour and minute drop-down lists.
Job Info	
Job Description	Enter the Job Description. Make each description unique so you can easily identify jobs. This is mandatory.
E-mail	Enter e-mail addresses to which the job will send status notices. Separate multiple addresses with commas or semicolons. You must configure the SMTP server to send e-mails (**Common Services > Server > Admin > System Preferences**). If the user who has created the job has a valid e-mail address, an e-mail notification is sent with the user's address in the sender address field, when job is started and completed. If the user who has created the job does not have a valid e-mail address, then the notification e-mails will be sent with the sender address field blank. Notification e-mails include a URL that displays the job details (see Viewing Job Details for the more information about what details are displayed). If you are not logged in, you must log in using the provided login panel to view the job details.
Comments	Enter your comments for the job. Comments appear in job work order and are stored in configuration archive.

Field	Description
Approver Comments	Enter comments for the job approver. This field is displayed only if you have enabled job approval for NetConfig. For more details the section Enabling Approval and Approving Jobs Using Job Approval.
Maker E-mail	Enter the e-mail-id of the job creator. This field is displayed only if you have enabled job approval for NetConfig. This is a mandatory field. For more details the section Enabling Approval and Approving Jobs Using Job Approval.

Step 10 Set the job options, in the Job Options pane.

Field	Description
Fail on Mismatch of Config Versions	Select to cause job to be considered a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.
Sync Archive before Job Execution	Select to cause job to archive running configuration before making configuration changes.
Copy Running Config to Startup	Select to cause job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. Does not apply to Catalyst OS devices.
Enable Job Password	
Login Username	Enter the Login Username. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of Common Services.
Login Password	Enter the job password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of Common Services.
Enable Password	Enter the Enable password. This option is available to you if you have set the appropriate job password policy in the Configuration Management module. This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module of Common Services.

Field	**Description**
Failure Policy	Select one of these options to specify what the job should do if it fails to run on a device. • Stop on failure: If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully. • Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices. The database is updated only for the devices on which the job was executed successfully. • Rollback device and stop—Rolls back the changes on the failed device and stops the job. • Rollback device and continue—Rolls back the changes on the failed device and continues the job. • Rollback job on failure—Rolls back the changes on all devices and stops the job. Roll back configuration changes to failed device or all devices configured by job (see Configuring a Job to Roll Back on Failure.)
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. • Sequential—Allows the job to run on only one device at a time. If you select sequential execution, you can click **Set Device Order** to set the order of the devices. In the Device Ordering dialog box: **a.** Select a device name **b.** Click **Move Up** or **Move Down** to change its place in the order. **c.** Click **OK** to save the current order and close the dialog box or Click **Cancel** to close the dialog box without making any changes.

Step 11 Click **Device Order** to view the device order. The Set Device Order pop-up appears.

You can reset the order in which the job should be executed on the devices using the up and down arrows. When you are done, click **Done**. The pop-up closes.

Step 12 Click **Next**.

The Job Work Order dialog box appears with the general information about the job, the job policies, the job approval details (if you have enabled job approval), the device details, the task, and the CLI commands that will be executed on the selected devices as part of this job.

A sample work order:

```
-----------------------------------------------------------------

General Info

Owner: admin

Description: test job for documenting the workflow
```

```
Schedule Type: Run Once

Schedule Time: Mon Aug 22 12:45:00 IST 2011

--------------------------------------------------------------------

Job Policies

Failure Policy: Ignore failure and continue

E-mail Notification: Disabled

Execution Policy: Sequential

Fail on Mismatch of Config Versions : Disabled

Copy Running Config to Startup: Disabled

Sync Archive before Job Execution : Disabled

Job Password: Disabled

------------------------------------------------------------------

Job Approval Details

Job Approval: Disabled

------------------------------------------------------------------

Device Details

Device: 10.76.38.14

Task: Banner

Commands:

banner motd "welcome"

------------------------------------------------------------------
```

Step 13 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A notification message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

Browsing and Editing Jobs Using the NetConfig Job Browser

You can browse the NetConfig jobs that are registered on the system. Using the NetConfig Job Browser dialog box you can also manage NetConfig jobs using the job browser. That is, you can edit, copy, retry, stop, or delete jobs using this job browser.

To create and start a new NetConfig job, see Starting a New NetConfig Job.

Note View Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To invoke the NetConfig job browser:

Select **Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs**.

The NetConfig job browser dialog box appears with a detailed list of all scheduled report jobs.

The columns in the NetConfig job browser dialog box display the following information:

Column	Description
Job ID	Unique number assigned to job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the hyperlink to view the Job details (see Viewing Job Details).
Status	Status of the job: • Successful—When the job is successful. • Failed—When the job has failed. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. This count of failed devices is not displayed for jobs restored from RME 4.0.4 or lesser versions. • Cancelled—When the job has been stopped. • Running—When the job is in progress. • Waiting—When the job is waiting approval (if job approval has been enabled). • Rejected—When the job has been rejected (if job approval has been enabled).
Description	Description of the job, entered at the time of job creation.
Owner	Username of the job creator.
Scheduled at	Date and time at which the job was scheduled.
Completed at	Date and time at which the job was completed.
Schedule Type	Type of job schedule—Immediate, Once, Daily, Weekly, Monthly, Last day of the month. You can specify when you want to run the NetConfig job. To do this, select one of these options from the drop down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. • Last Day of the Month—Runs the job on the last day of the month, beginning with the month that you specify. For periodic jobs, the subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

Using the Filter by field in the NetConfig Job Browser, you can filter the jobs displayed in the browser.

You can filter the jobs displayed in the NetConfig Job Browser using any of the following criteria and clicking **Filter**:

Filter Criteria	**Description**
All	Select All to display all jobs in the job browser
Job ID	Select Job ID and enter the Job ID (s) that you want to display. For non-periodic job, the specified Job ID appears in the browser, for periodic jobs, all the instances of the selected Job ID will also be displayed in the browser.
Status	Select Status and then select any one of these: • Successful • Failed • Cancelled • Running • Scheduled • Approved • Waiting • Rejected
Description	Select Description and enter the first few letters or the complete description.
Owner	Select Owner and enter the user ID or the beginning of the user ID.
Schedule Type	Select the schedule type and select any one of these: • Immediate • Once • Daily • Weekly • Monthly • Last day of the month

Records for NetConfig jobs need to be purged periodically. You can schedule a default purge job for this purpose. For more details see the topic Job Purge in the section Setting System-wide Parameters Using System Preferences.

Refresh (Icon)	Click on this icon to refresh the NetConfig job browser.

You can perform the following operations using the NetConfig job browser:

Table 9-2 NetConfig Job Browser Operations

Button	**Description**	**Usage Notes**
Edit	Edits selected pending job. The Job definition opens at the Devices and Tasks dialog box, with current information. You can edit a job the same way you define and schedule a new job (see Starting a New NetConfig Job). The Job ID of an edited job remains unchanged.	Unless you own job, your login determines whether you can use option. If job start time occurs during editing, it runs without edits. You can complete edits and schedule job to run again, but you cannot reedit job. To prevent job from running without edits, do one of the following: • Complete your edits before job start time. • Cancel job and create a new one.
Copy	Copies selected job. You can copy a job and give it a new schedule. The Job definition opens at the Devices and Tasks dialog box, with all your selections for the job that you are copying. You can edit the copied job in the same way you define and schedule a new job (see Starting a New NetConfig Job). A new Job ID with the copied job details is created.	-
Retry	Retry a failed job. The Job definition opens at the Devices and Tasks dialog box. You can edit the job the same way you define and schedule a new job, except that you cannot add new devices or change the tasks for the job that you are retrying. You can, however, select a few number of failed devices to retry the job.	Unless you own the job, your login determines whether you can use this option. There may be some devices whose configuration has been downloaded however their running configuration has not been written to the Startup configuration. You can perform Retry Job on these devices just as you can on a failed job.

Table 9-2 NetConfig Job Browser Operations (continued)

Button	Description	Usage Notes
Stop	Stops or cancels a running job. You can stop/cancel a running job. You will be asked to confirm the cancellation of the job. However, the job will be stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state. If the job that you want to stop is a periodic job, you will also be asked whether you want to cancel all the instances of the job. Click **OK** to cancel all instances. If you click **Cancel**, only the selected instance of the job is cancelled. The next instance of the job will appear in the Job browser with the status `Scheduled`.	Unless you own the job, your login determines whether you can use this option. You cannot re-start the stopped job. You can however copy the stopped job and Job ID.
Delete	Deletes the selected job from the job browser. You can select more than one job to delete. You will be asked to confirm the deletion. If the job that you have selected for deletion is a periodic job, this message appears: `If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue?` Click **OK** to confirm the deletion. The job, and its instances will be deleted. You can delete a job that has been successful, failed, or stopped, but you cannot delete a running job.	Unless you own the job, your login determines whether you can use option. You must stop a running job before you can delete it.

Viewing Job Details

From the Job Browser dialog box, you can learn more about any job by viewing its details.

Step 1 Go to the NetConfig Job Browser, click the Job ID hyperlink. (See Starting a New NetConfig Job to invoke the NetConfig Job Browser.)

The Job Details pop-up appears, displaying the day, date and time details in the header at the top of the report. The Job ID and the Status appear in the header of the report.

The Job Details dialog box has two panes. The left pane contains a table of contents for the job results. The results appear in the right pane.

Step 2 Click a page in the left pane to view its corresponding report in the right pane.

Double-click a folder in the left pane to open and close it.

If the folder has subfolders, the next level of subfolders appears under it. Otherwise, its corresponding report appears in the right pane.

The contents of the left pane depends on the state of the job. The left pane can contain:

- Download Summary (in the Job Details folder).
- Downloaded Devices (in the Device Details folder).
- Work Order

Page/Folder	Description	
Job Details	Download Summary	Click to display summary of completed job: • Download Summary: – Status – Start Time – End Time • Job Messages: – Pre-job Execution – Post-job Execution • Device Update: – Successful – Failed – Not attempted – Pending

Page/Folder	**Description**	
Device Details	Downloaded Devices	Contains detailed job results for each device in a table: • Device—List of devices on which the job ran. • Status—Status of job (success, failure, etc.) • Message—For example, if the job failed on the device, the appropriate reason for failure is displayed. If the job was a success on that device, the message "Download Successful" is displayed. You can filter the devices by selecting a status and clicking **Filter**. This page displays the number of rows you have set for display in the Rows per page field. You can increase the rows up to 50 per page. You can navigate between the pages of the report using the navigation icons at the right bottom of this table. Click on a device to view the details such as protocol, status and reason when applicable, task used and the CLI output for that device. These details appear in a pop-up window. Double-click to display status folders that correspond to possible device status.
	StatusFolder	**Description**
	Update Successful	Devices were successfully updated
	Update Failed	Devices were not successfully updated. Includes devices on which rollback was attempted, regardless of whether it was successful.
	Not Attempted	Job did not try to update devices, even though they were selected. Usually occurs when a previous device failed and failure property was set to Stop on Failure.
Work Order	Click to display Job Work Order, which contains same the information as the workorder that was displayed when the job was created. (For the workorder details, see Step 12 in Starting a New NetConfig Job). For retried jobs, the job definitions are not updated. For such jobs, the original job definitions are retained.	

To perform actions, click one of the following (For detailed descriptions of these operations see Table 9-2NetConfig Job Browser Operations in Table 9-2):

- Edit
- Copy
- Retry`
- Stop
- Delete

Setting Job Approvers

If required, you can enable job approval for NetConfig jobs.

For more details see the topic Setting Up Job Approval in the section Enabling Approval and Approving Jobs Using Job Approval.

Configuring Default NetConfig Job Policies

Ensure that you have configured the default job policies for NetConfig jobs.

For more details see the topic Configuring Default Job Policies in the section Archiving Configurations and Managing Them Using Archive Management.

Password Policy for NetConfig Jobs

Ensure that you have set the password policy for NetConfig jobs. For more details see the topic Configuring Default Job Policies in the section Archiving Configurations and Managing Them Using Archive Management.

Setting the Transport Protocol Order for NetConfig Jobs

Ensure that you have set the Transport protocol order for your job using **Resource Manager Essentials > Admin > Config Mgmt**. For more details see the topic Configuring Transport Protocols in the section Archiving Configurations and Managing Them Using Archive Management.

Creating and Editing User-defined Tasks

You can create User-defined Tasks and add one or more templates to each task.

The template, in turn, is associated with the Meta-Data Framework (MDF) categories of devices, for which these templates will be applicable.

The templates contain configuration commands and rollback commands (see Creating Rollback Commands). You can enter the configuration commands either by typing them or by importing them from a file.

You can create a new task and add one or more templates to it. You can also add templates to an existing task. You name a task when you create it, and it is saved for future use. You can copy, edit, and reuse your tasks. You can assign access privileges to tasks while or after you create them (seeAssigning Tasks to Users).

You cannot add User Defined Templates to System Defined Tasks.

After you successfully create a User-defined Task, this task will appear in the Task Selector of the NetConfig Job creation wizard, and you can create a job using the task. For details on the Task Selector and job creation, see Step 2 in Starting a New NetConfig Job.

For each template, you should specify all the information including the configuration commands, rollback commands (seeRolling Back Configuration Changes), mode (Config or Enable), and the device category for which these commands will be applicable.

At the time of job creation, you should ensure that the user-defined task that you have selected is applicable to the MDF categories of the devices that you have selected.

If the task that you have selected does not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane of the NetConfig job wizard, during job creation.

For example, if you have selected an CatalystOS category of device, but selected a user-defined task that is applicable to a Cable device, then the task will not show up in the Applicable Tasks pane of the job wizard and you will not be able to proceed further with the job creation. For details on the Applicable Tasks pane and job creation, see Step 5 in Starting a New NetConfig Job

⚠ **Caution** NetConfig does not validate the commands you enter in a user-defined template within a task. If you enter incorrect commands you might misconfigure or disable the devices on which jobs using the template run.

View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Config Mgmt > NetConfig > User-defined Tasks**.

The User-defined Tasks dialog box appears. If you are creating a task for the first time, the system displays a message that there are no user-defined tasks.

The User-defined Tasks dialog box has a Tasks browser in its left pane. After you create a task, the task is displayed in the Tasks browser along with its template(s).

Step 2 Define or edit a user-defined task by entering the following information in the dialog box:

Area/Field/Button	Description	Usage Notes
Name	Enter name for the new task. This is a mandatory field.	To create new task from a copy of an existing task: 1. Select the name from Templates list, 2. Enter the new name. 3. Save the task. To modify a task, select it from the tasks list but do not modify its name. You can modify a task by adding or deleting templates, modifying existing templates and changing other details.
Template Name	Enter the template name. This is a mandatory field.	Template Name is provided for User Defined Tasks when you create a template for more than one device category which has different commands to execute.
Command Mode	Select mode (config or enable) in which commands will run.	Each user-defined template can run commands in one mode only. If you select **Enable**, enter Rollback Commands area is disabled because only config commands can be rolled back.

Area/Field/Button	**Description**	**Usage Notes**
Parameterized	Select Parameterized if you want to create a parameterized template.	The template parameters will be picked up from a file that you specify, at the time of scheduling a job using this task. See “Parameterized Templates”.
Device Type	Select device category template will configure.	You can associate any number of MDF categories with a template, if the command is applicable to them.
CLI Commands	Enter configuration commands or select the configuration commands file. The configuration commands file should reside in the default location: On Solaris: /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: *NMSROOT*\files\rme\netconfig\cmdFiles Where, *NMSROOT* is the CiscoWorks install directory. If you want to import the configuration commands from an existing file, enter the default file location in the Import from File field. Alternatively, when you click on the Browse button, a file browser opens with the default location of the configuration commands file. You cannot change this default import directory.	To enter configuration commands, do any of the following: • Type in larger text box, one per line. Or • Enter enter the default file location of the configuration command files in the Import from File field. • Click **Browse.** A file browser opens with the default location of the configuration commands file. You cannot change this default import directory. You can also enter interactive commands and multi-line commands. See: • Handling Interactive Commands

Area/Field/Button	Description	Usage Notes
Rollback Commands	Enter configuration commands for the template to run when the job fails and the failure policy is set to the rollback option. If you want to import the rollback commands from an existing file, enter the file location in the Import from File field. The rollback commands file should reside in the default location: On Solaris: /var/adm/CSCOpx/files/rme/netconfig/cmdFiles/ On Windows: *NMSROOT*\files\rme\netconfig\cmdFiles Where, *NMSROOT* is the CiscoWorks install directory. Alternatively, when you click on the Browse button, a file browser opens with the default location of the rollback commands file. You cannot change this default import directory.	To enter rollback commands, do any of the following: • Type in larger text box, one per line. • Enter enter the default file location of the rollback command files in the Import from File field. • Click **Browse.** A file browser opens with the default location of the configuration commands file. You cannot change this default import directory.

- Click **Save** to save the task with the current information.

  Or
- Click **Delete** to delete the current task from the system.

To cancel the user-defined task you are creating, select a command from the Jobs or Admin menu (or a corresponding button) and click **Yes** in the resulting dialog box.

To add a user-defined task, select Select **Resource Manager Essentials > Config Mgmt > NetConfig > User-defined Tasks**. The User-defined Tasks dialog box appears with no values.

To copy a user-defined task:

Step 1 Select the task from the Tasks browser.

The details appear in the right pane of the User-defined Tasks dialog box.

Step 2 Change the name of the Task and click **Save**.

To modify a user-defined task:

Step 1 Select the task from the Tasks browser.

The details appear in the right pane of the User-defined Tasks dialog box.

Step 2 Select templates associated with the task from the Task browser, and modify them

You can change details such as the command mode, parameterization option, the device type, the CLI commands or the rollback commands.

You can add a template or delete an existing one. When you click Save, a message appears that the task is modified.

Parameterized Templates

You can include parameterized templates within User-defined tasks. A parameterized template allows the configuration commands in the templates to contain user-defined variables.

Multiline feature of parameterized templates is not supported. However, interactive command deploy is supported.

You can select the Parameterized option when you create a User-defined task (see Creating and Editing User-defined Tasks).

If you select the Parameterized option, you should enter the actual values for the parameters in the template in a separate Parameters file (see Creating a Parameters File (XML file)) when you create a NetConfig job (see Creating and Editing User-defined Tasks). The Parameters file is the XML file that contains the parameter values.

The Parameters file should reside on the server at this location:

NMSROOT\files\rme\netconfig\cmdFiles

where *NMSROOT* is the RME install directory.

To create a Parameterized User-defined task and apply this in a NetConfig job:

Step 1 Create a User defined Task with variables embedded in the command body. For details see Creating and Editing User-defined Tasks.

For example:

You can enter the command **`ntp server`** *`$ntpServer`* in the CLI Commands text box in the User-defined Tasks dialog box. Commands

Step 2 Select the Parameterized check box in the User-defined Tasks dialog box.

Step 3 Click **Save** to save your User-defined Parameterized task.

Step 4 Create the Parameters file (XML file) containing the values for *`$ntpServer`* task. For details, see Creating a Parameters File (XML file).

For example:

```
<DEVICE NAME = 10.76.38.54>

<CMDPARAM NAME = ntpServer>

<value>mytimeserver</value>

</CMDPARAM>

</DEVICE>
```

Step 5 Repeat the above step in the Parameters file, for all the devices that you plan to include in the job, if each device refers to a different *`ntpServer`*.

Alternatively, you can have a global section if that variable does not change for each device. For details, see Creating a Parameters File (XML file).

Step 6 Store the Parameters file in *NMSROOT*\files\rme\netconfig\cmdFiles directory (where *NMSROOT* is the RME install directory).

Step 7 Create a NetConfig job and select your User-defined Parameterized task. For details see Starting a New NetConfig Job.

You are prompted to enter the filename while adding the task to the NetConfig job.

You can check the syntax of the text file that contains the parameters. To do this, select **Check Syntax**.

Step 8 Complete the job creation. For details, see Creating and Editing User-defined Tasks.

Creating a Parameters File (XML file)

A specific format is defined for embedding variables in User-defined tasks and the corresponding Parameters file that contains the values for the parameters.

The variables in the User-defined tasks, which you enter in the CLI Commands text area of the User-defined Tasks dialog box (see Creating and Editing User-defined Tasks), should be preceded by `$`.

For example, for an NTP server parameter, it should be: `$ntpServer`

Similarly, the Parameters file also follows a specified format.

Here is the sample format and example of the Parameters file (the XML command file that contains the values for the parameters) for a parameterized template:

```
<GLOBAL>

<CMDPARAM NAME = password>

<value>abc</value>

</CMDPARAM>

<CMDPARAM NAME = message>

<value>test all</value>

</CMDPARAM>

</GLOBAL>


<DEVICE NAME = 10.76.38.54>

<CMDPARAM NAME =  ntpServer>

<value>ServerName</value>

</CMDPARAM>

</DEVICE>
```

You can assign the device-specific values to variables in the `<DEVICE>` area. If there are no device-specific values, the default values in the `<GLOBAL>` area are considered as actual values for these variables. You do not need to add a `<GLOBAL>` area in the Parameters file if you are referencing each device explicitly (using the `<DEVICE>` area for each device).

Parameters File: More Examples

This section gives more examples of the format of the text to be entered in the CLI Commands body at the time of creating a User-defined Task, and the commands to be entered in the corresponding Parameters file.

For example, you can enter these parameters while creating a User-defined task, in the CLI Commands text box:

```
ntp server ntpServer
ip http port portValue
ip address ipAddress
```

In the corresponding Parameters file, which is stored under *NMSROOT*\files\rme\netconfig\cmdFiles, (where *NMSROOT* is the RME install directory) enter:

```
<GLOBAL>
<CMDPARAM NAME = ntpServer>
<value>10.10.10.10</value>
</CMDPARAM>
<CMDPARAM NAME = portValue>
<value>90</value>
</CMDPARAM>
<CMDPARAM NAME = ipAddress>
<value>1.1.1.1</value>
</CMDPARAM>
</GLOBAL>

<DEVICE NAME = 10.76.38.54>
<CMDPARAM NAME = ntpServer>
<value>20.20.20.20</value>
</CMDPARAM>
<CMDPARAM NAME =  portValue>
<value>55</value>
</CMDPARAM>
</DEVICE>

<DEVICE NAME = 10.77.202.229>
<CMDPARAM NAME = ntpServer>
<value>30.30.30.30</value>
</CMDPARAM>
</DEVICE>
```

In such a case, when the NetConfig job contains the device 10.76.38.54, the following commands are generated:

`ntp server 20.20.20.20` (taken from the device-specific section of the Parameters file)

`ip http port 55` (taken from the device-specific section of the Parameters file)

`ip address 1.1.1.1` (taken from the global section of the Parameters file)

When the job contains the device 10.77.202.229, the following commands are generated:

`ntp server 30.30.30.30` (taken from the device-specific section of the Parameters file)

`ip http port 90` (taken from the global section of the Parameters file)

`ip address 1.1.1.1` (taken from the global section of the Parameters file)

When the job contains any other devices, all the values are taken from the global section of the XML file, and the following commands are generated:

```
ntp server 10.10.10.10
ip http port 90
ip address 1.1.1.1
```

If the value for a parameter is not found in the command file, the syntax check (in the job creation flow) displays an error.

Note You can enter any special character that is accepted by the device as the value for a parameter in the command file. This is because NetConfig does not process the parameter values. NetConfig only reads the value given between `<value>` and `</value>` tags and generates the command. Therefore, you can enter any special character that the device accepts.

Assigning Tasks to Users

You can assign access privileges to NetConfig tasks, to users with Network Operator privileges or lesser. All other users with privileges higher than Network Operator are assigned all tasks by default.

A network administrator must assign task access privileges to other users. See Understanding NetConfig User Permissions section for details.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To assign tasks to users:

Step 1 Select **Resource Manager Essentials > Config Mgmt > NetConfig > Assigning Tasks**.

The Assign Tasks dialog box appears.

Step 2 Enter the username of the user to whom you want to assign the tasks.

This should be a valid CiscoWorks user. If RME has been registered with a Cisco Secure ACS Server, then the user should be a valid ACS user.

Step 3 Select the task that you want to allocate to the user from the Available tasks list box and click **Add**.

You can select more than one task, by holding down the Shift key while selecting the task.

The selected tasks appear in the Selected Tasks list box.

To remove assigned tasks, select the tasks from the Selected Tasks list box and click **Remove**.

Step 4 Add all the required tasks to the Selected Tasks list box.

Step 5 Click **Assign** to assign the task access privileges to the specified user.

For a specified user, to see the assigned tasks, enter the username in the Username field and click **Show Assigned**.

The tasks assigned to the user appear in the Selected Tasks list box.

Handling Interactive Commands

An interactive command is the input you will have to enter, following the execution of a command.

For example, on a Catalyst device, a clear counters command on a Cat 5000 will give the following output:

```
c5000# (enable) clear counters. This command will reset all MAC and port counters reported
in CLI and SNMP. Do you want to continue (y/n) [n]?
```

In RME, such commands can be included in config jobs executed via NetConfig or ConfigEditor. For more details also see Editing and Deploying Configurations Using Config Editor.

You can handle interactive commands using NetConfig user-defined templates, and by using Adhoc tasks. See Using NetConfig User-defined Templates and Adhoc Tasks.

You cannot run interactive commands through NetConfig CLI.

Using NetConfig User-defined Templates and Adhoc Tasks

You can enter an interactive command in the Enter CLI Commands area, using the following syntax:

CLI Command`<R>`*command response 1* `<R>`*command response 2*

`<R>` tag is case-sensitive and this must be entered in uppercase only.

Example

For a Catalyst device, a **`clear counters`** command will give the following output

```
c5000# (enable) clear counters This command will reset all MAC and port counters reported
in CLI and SNMP. Do you want to continue (y/n) [n]?

To clear the counter, the syntax is:

clear counters <R>y

To accept the default, the syntaxes are:

clear counters <R>n

or

clear counters <R>
```

To accept the default value, you do not need o enter any values after the tag `<R>`.

Handling Multi-line Commands

You can enter multi-line commands as a part of User-defined and Adhoc tasks. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>.

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space.

Example

```
<MLTCMD> banner login "Welcome to

CiscoWorks Resource Manager

Essentials - you are using

Multi-line commands" </MLTCMD>
```

You can have a blank line within a multi-line command. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device.

Using System-defined Tasks

NetConfig provides you with system-defined configuration tasks. You can create configuration commands using task GUI (see Understanding the System-defined Task User Interface (Dialog Box)).

Each task supports one or more device categories (see Table 9-3). Table 9-3 also provides you with a comprehensive list of all the templates available, and a brief description of each.

The devices and the system-defined tasks as available in the Devices and Tasks dialog box of the NetConfig job wizard. After you select devices and the tasks, and click **Next** (see Starting a New NetConfig Job), the selected tasks appear in the Applicable Tasks pane of the Add Tasks dialog box (in the Job wizard).

When you select an applicable task and then click **Add Instance**, a dialog box opens for the selected system-defined configuration task.

This is a dynamic user interface. The task dialog box displays parameters based on your device selection in the Device Selector.

For example, if you have selected IOS devices, you will be able to specify IOS parameters in this dialog box. If not, this section will not be available to you.

When you enter information in the fields of the task and click **Save**, the task appears as a numbered instance in the Added Instances pane of the Add Tasks dialog box.

For the detailed procedure, and also for information on how to edit the task instances, view CLI, or delete the instances, see Starting a New NetConfig Job.

You can add multiple instances of a configuration task to a job by selecting an applicable task, adding information and saving the information each time. However, you can include only one instance of a task in a job.

Each system-defined task also creates rollback commands (see) that you can use to roll back the changes to devices if the job fails.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

Table 9-3 NetConfig System-Defined Tasks Supported by the RME 4.1 Device Categories

Task	Description	IOS	Cat OS	CSS	CE	NAM	PIX	Cable
Adhoc (See Adhoc Task.)	Enter any configuration commands as required.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication Proxy (See Authentication Proxy Task.)	Configure Authentication Proxy.	Yes	-	-		-	-	Yes
Banner (See Banner Task.)	Add, remove, or edit banners.	Yes	Yes	-		-	-	Yes
CDP (See CDP Task.)	Configure Cisco Discovery Protocol (CDP).	Yes	Yes	-	Yes	-	-	Yes
Certification Authority[1] (See Certification Authority Task.)	Create, or modify Certification Authority. Provides manageability and scalability for IP security (IPSec) standards on VPN devices.	Yes	-	-		-	-	Yes
CryptoMap[1] (See Crypto Map Task.)	Configure IPSec.	Yes	-	-	-	-	Yes	Yes
DNS (See DNS Task.)	Configure DNS.	Yes	Yes	Yes	Yes	Yes	-	Yes
Enable Password (See Enable Password Task.)	Configure, or change enable or secret password to enter in the enable mode on devices.	Yes	Yes	-	-	-	Yes	Yes
HTTP Server (See HTTP Server Task.)	Configure HTTP access on VPN devices.	Yes	Yes	-	-	-		Yes
IKE Configuration[1] (See Internet Key Exchange (IKE) Configuration Task.)	Configure IP security (IPSec).	Yes	-	-	-	-	Yes	Yes
Local Username (See Local Username Task.)	Configure local username and password authentication on devices.	Yes	-	Yes	-	-	-	Yes
NTP (See NTP Server Configuration Task.)	Configure Network Time Protocol (NTP).	Yes	Yes	Yes	Yes	-	-	Yes
Radius Server (See RADIUS Server Configuration Task.)	Configure RADIUS server and task.	Yes	-	Yes	Yes	-	-	Yes
RCP RCP Configuration Task	Configure rcp	Yes	-	-	-	-	-	Yes
Reload Reload Task	Reload devices	Yes			Yes	Yes		Yes
SNMP Community SNMP Community Configuration Task	Add, remove, and edit SNMP community strings	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Security SNMP Security Configuration Task	Configure SNMP Security feature on devices.	Yes	-	-	Yes	-	-	Yes

Table 9-3 NetConfig System-Defined Tasks Supported by the RME 4.1 Device Categories (continued)

Task	Description	IOS	Cat OS	CSS	CE	NAM	PIX	Cable
SNMP Traps Management SNMP Traps Configuration Task	Configure SNMP traps.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSH SSH Configuration Task	Configure SSH.	Yes	-	Yes	Yes	Yes		Yes
Syslog Syslog Task	Configure syslog message logging.	Yes	Yes	Yes	Yes	-	Yes	Yes
TACACS TACACS Configuration Task	Configure TACACS authentication.	Yes	-	-		-	-	Yes
TACACS+ (See TACACS+ Configuration Task.)	Configure TACACS+ authentication	Yes	Yes	-	Yes	Yes	-	Yes
Telnet Password (See Telnet Password Configuration Task.)	Add, remove, and edit Telnet passwords	Yes	Yes	-	-	-	Yes	Yes
Transform Set (See Transform System-Defined Task.)	Configure IPSec.	Yes	-	-	-	-	Yes	Yes
User Defined Protocol (See Use-defined Protocol Task.)	Configure the user-defined protocol on NAM devices.	-	-	-	-	Yes	-	-
Web User (See Web User Task.)	Configure the web user for NAM devices	-	-	-	-	Yes	-	-
BPI/BPI+ (See Cable BPI/BPI+ Task.)	Assign self-signed certificate, configure cable interface, and set BPI/BPI+ options.	-	-	-	-	-	-	Yes
Interface Bundle[2] (See Cable Interface Bundling Task.)	Configure Interface Bundling on selected cable interface.	-	-	-	-	-	-	Yes
Cable DHCP-GiAddr and Helper[2] (See Cable DHCP-GiAddr and Helper Task.)	Configure DCHP-GiAddr and Helper Address of the selected cable interface.	-	-	-	-	-	-	Yes
Cable Downstream[2] (See Cable Downstream Task.)	Activate/Deactivate DS Ports, Interleave Depth, MPEG Framing Format, Modulations, Channel ID and Frequency of the selected cable interfaces.	-	-	-	-	-	-	Yes
IGMP[2] (See IGMP Configuration Task.)	Configure IGMP of selected cable interfaces.	-	-	-	-	-	-	Yes
Interface IP Address (See Interface IP Address Configuration Task.)	Configure IP interface address of selected interface.	-	-	-	-	-	-	Yes

Table 9-3 NetConfig System-Defined Tasks Supported by the RME 4.1 Device Categories (continued)

Task	Description	IOS	Cat OS	CSS	CE	NAM	PIX	Cable
Cable Spectrum Management (See Cable Spectrum Management Task.)	Assign Spectrum Groups and Interfaces on a selected cable interface.	-	-	-	-	-	-	Yes
Cable Trap Source (See Cable Trap Source Task.)	Configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.	-	-	-	-	-	-	Yes
Cable Upstream[2] (See Cable Upstream Task.)	Activate and configure upstream on selected cable interfaces.	-	-	-	-	-	-	Yes

[1] You must follow this sequence to complete the configuration of the IPSec on devices:

1) IKE configuration system-defined task.

2) Transform system-defined task.

3) Crypto Map system-defined task.

[2] At a time, you can apply this task only to a single device, because cable templates configure interfaces on devices.

Understanding the System-defined Task User Interface (Dialog Box)

NetConfig tasks support devices in the following device categories:

- IOS
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS
- Cable

Each of the system-defined tasks have their own dynamic user interface, or dialog box, that displays fields for a specified category of devices only if you have selected that category of device.

The dialog boxes for system-defined tasks may have these groups, links, and buttons:

- Common Parameters—This group of fields appears at the top of the task dialog box. In the fields under this group, you can enter the parameters that are common to all the categories of devices that you have selected.
- Device Category-specific Parameters—This group of fields is specific to a device category. If, for a specified device category, only the common parameters are applicable, this message appears in the user interface:

  ```
  No Category-specific Commands
  ```

- Applicable Devices—This link is available in the device category-specific group of fields and enables you to view the devices in your selection, to which the device-specific parameters apply.
- Buttons in the system-defined tasks interface:

Button	Action
Save	Saves the information that you have entered in the fields in the task dialog box.
Reset	Clears all the fields.
Cancel	Cancels your changes, and closes the task dialog box.

For the cable devices, you can apply a task only to a single device at a time, because cable templates configure interfaces on devices.

Also, for the cable tasks to work correctly, you must have valid SNMP credentials in Device and Credential Repository (DCR). See Adding and Troubleshooting Devices Using Device Management for more information on setting valid SNMP credentials.

Therefore, if you have selected more than one cable device and selected tasks for them, the task may not appear in the Applicable Tasks pane of the Add Tasks dialog box. For the tasks that are applicable to cable devices, see Table 9-3.

Understanding the NetConfig Credentials Configuration Tasks

NetConfig provides for tasks to configure credentials on devices. These tasks are:

- Enable Password (See Enable Password Task.)
- Local Username (See Local Username Task.)
- Radius Server (See RADIUS Server Configuration Task.)
- TACACS TACACS Configuration Task
- TACACS+ (See TACACS+ Configuration Task.)
- SNMP Community (See SNMP Community Configuration Task.)
- SNMP Security (See SNMP Security Configuration Task.)

The credential store allows only one set of login credentials per device - Primary username and primary password, irrespective of the authentication type.

Hence, this imposes certain limitations on the NetConfig templates, especially, when you are configuring/modifying the authentication method on the device.

To overcome this, an option to specifically update the credential store is provided in the credential tasks. The credential store is updated only when this option is chosen with the values specified.

The usage of NetConfig credentials tasks to configure the credentials on a device should be based on the active credentials (e.g. Telnet, TACACS, etc.) in the device. For example if the device is configured with TACACS+, you should use only TACACS+ template to configure the credentials.

Example

When you remove the TACACS+ authentication for the device, the device reverts to the authentication method that was earlier configured on it. For example, the local username.

However, RME is unaware of the fallback authentication method, and the respective credentials. If Device and Credential Repository is not updated with the right credentials, the subsequent device operations from RME will fail.

In this case, you should select the option to update the local credential store and specify the local username credentials. When the job runs, NetConfig updates Device and Credential Repository with this set of credentials, so that for subsequent devices, access from RME will be successful.

Adhoc Task

You can use the Adhoc system-defined task to add configuration commands to a job, during job definition.

You cannot save an instance of an Adhoc task, for future use. If you need to reuse a template that provides capabilities unavailable from the system-defined tasks, you can create a user-defined tasks (see Creating and Editing User-defined Tasks).

Caution NetConfig does not validate commands you enter in the Adhoc task. If you enter incorrect commands, you might misconfigure or disable devices on which jobs that use the task run.

Groups for each of device categories that you have selected, appear in the Adhoc Configuration dialog box. To invoke the Adhoc Configuration dialog box, see Starting a New NetConfig Job.

You can enter configuration and rollback commands for these device categories:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 9-3.

Note As Cable devices fall under the IOS category, you can enter adhoc commands in the IOS group of fields in the Adhoc Configuration dialog box.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Adhoc Configuration dialog box are:

Group	Field	Description
Commands	CLI Command	Enter configuration commands. You can also enter interactive commands (see Handling Interactive Commands) and multi-line commands see Handling Multi-line Commands).
	Rollback Command	Enter rollback commands.
Command Mode	Config or Enable	Select the mode (config or enable) in which the task configuration commands will run. If you have selected Catalyst OS, or NAM devices, then the enable mode is preselected, and you do not have the option to select the config mode.

If you enter any credential command in the CLI Commands or Rollback Commands fields, then those credentials will be masked in the job work order and the job results page.

For example, the command, **`snmp-server community public ro`** will be displayed as **`snmp-server community ***** ro`**.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Authentication Proxy Task

The Authentication Proxy feature helps users to log into the network or access the Internet using HTTP. Their specific profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server.

The Cisco Secure Integrated Software authentication proxy feature allows network administrators to apply specific security policies on a user to user basis. You can use the Authentication Proxy system-define, configuration Task on IOS devices which have been configured for VPN functionality.

The IOS category of devices (including Cable devices) are supported by this task.

For more details, see Table 9-3.

You can enter the details of this task in the Authentication Proxy Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Authentication Proxy Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters	Authorization (AAA)	Action	Select the required option to enable, disable or make no change to the authorization configuration.
		Method 1	Select either tacacs+ or radius as your first method of authorization.
		Method 2	Select either tacacs+ or radius as your second method of authorization, based on your selection in the first method
	Cache Timeout	Minutes (1-2147483647)	Timeout value. The default timeout value can be in the range of 1 and 2,147,483,647.
		Set to default	Select this to set the default cache timeout value of 60 seconds.
	Banner	Action	Select **Enable** or **Disable** to set or reset Banner display in the login page. • If you select **Enable**, the router name is displayed in the login page. • If you select **Disable**, then the router name is not displayed. If you do not want to make any changes to the banner, select **No Change.**

Group	Sub-Group	Field	Description
		Banner Text (Optional)	Enter the text that you want displayed in the banner. If you enter the banner text, then this text is displayed instead of the router name in the login page. This is an optional field.
	Authentication Proxy Rule	Action	Select **Enable** or **Disable** an authentication proxy rule. • If you select **Enable**, a named authentication proxy rule is created and associated with access list. • If you select **Disable**, the associated proxy rule is removed. Select **No Change** if you do not want to make changes to the Authentication Proxy Rule group of fields.
		Name	Enter a name for the authentication proxy rule. The name can be up to 16 alphanumeric characters.
		Overriding Timeout [optional(1-2147483647)]:	Enter a timeout value to override the default cache timeout. This is an optional field. The overriding timeout value should be in the range of 1 and 2,147,483,647.
		ACL Number/Name [optional]:	Enter a Standard Access list to be used with the Authentication proxy. This is an optional field.
	New Model	Action	Select to enable, disable, or make no change to new model state.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the numeric `56` or `K`*n*, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`.

Banner Task

You can use the Banner system-defined, configuration task to change banners on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 9-3.

You can enter the details of this task in the Banner Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Banner Configuration dialog box are:

Group	Sub Group	Field	Description
Common Parameters	Motd Banner	Action	Select the appropriate option to add or remove a message of the day banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
IOS Parameters	Exec Banner	Action	Select the appropriate option to add or remove an Exec banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
	Incoming Banner	Action	Select the appropriate option to add or remove an Incoming banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
	Login Banner	Action	Select the appropriate option to add or remove a Login banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
	Slip-PPP Banner	Action	Select the appropriate option to add or remove a Slip/PPP banner. Select **No Change**, if you are modifying an existing task, and you do not want to change the value in this field.
		Message	Enter message, if you selected **Add** in Action field.
CatOS Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

CDP Task

You can use the CDP system-defined task to configure Cisco Discovery Protocol (CDP) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine

For more details, see Table 9-3.

You can enter the details of this task in the CDP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the CDP Configuration dialog box are:

Group	Sub Group	Field	Description
Common Parameters	Run	Action	Select to enable, disable, or make no change to the CDP state.
	Hold Time	Seconds (10-255)	Enter holdtime in seconds. The CDP holdtime specifies how much time can pass between CDP messages from neighboring devices before the device is no longer considered connected and the neighboring entry is aged out. Value must be greater than value in Update Time field.
		Set to Default	Select this for the default hold time of 60 seconds
	Update Time	Seconds (5-254)	Enter time between CDP updates, in seconds. Value must be less than value in Hold Time field.
		Set to Default	Select this for the default update time of 60 seconds
	CDP Version	Run	Select the CDP Version (CDPv1 or CDPv2. CDP version 2 is the default value. If you are modifying the CDP Task and you do not want to change this field, select No Change.
IOS Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.
CatOS Parameters	Mod/Ports	Mod/Ports (Ex:2/1-12,3/5)	Enter modules and ports on which to enable or disable CDP. You can enter a single module and port or a range of ports, for example, 2/1-12,3/5-12.
		All mod/ports	Select to enable or disable CDP in all ports in all modules.
	CDP Format	Format	The options are: • No Change (Does not allow you to make any modifications to the specified CDP format.) • MAC • Other Select the required option.
CE Parameters	No category-specific commands.	-	This device category does not have any device-category-specific commands. Use the Common Parameters group to assign the values.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Certification Authority Task

You can use the Certification Authority (CA) system-defined configuration task to provide manageability and scalability for IP Security (IPSec) standards. The Certification Authority task can be used only on IOS devices configured for VPN functionality.

This task is applicable to IOS devices (including Cable devices).

For more details, see Table 9-3.

You can enter the details of this task in the Certification Authority Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use any CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Certification Authority Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters	Declare CA	Action	Select **Enable** or **Disable** to activate/deactivate Certification Authority (CA). • If you select **Enable** you can create or modify CA. • If you select **Disable**, you can delete the CA. Select **No Change**, to leave the CA Name unchanged.
		CA Name	Enter the CA name. This name is used to identify the certification authority to be configured. This name is the CA domain name.
	Enrollment URL	Action	• Select **Enable** to allow router to connect to the CA, using the URL specified in the Value field. • Select **Disable**, if you do not want to connect to the CA. • Select **No Change** to leave the Enrollment URL field unchanged.
		Value	Enter the URL of the CA. The URL should include any available non-standard cgi-bin script location.
	Enrollment Mode	Action	• Select **Enable** if the CA provides a Registration Authority (RA). • Select **Disable** to disable the specified LDAP Server. • Select **No Change** to leave the Enrollment Mode field unchanged.

Group	Sub-Group	Field	Description
		LDAP Server	Enter the LDAP server of the CA, if your CA system provides an RA. LDAP server contains the location of CRLs (certification revocation lists) and certificates.
	Enrollment Retry Period	Minutes [1- 60]	Enter the wait period between certification request retries. The wait period is between 1 to 60.
		Set to Default	Select this option to set the default wait period to 1 minute.
	Enrollment Retry Count	Number [1- 100]	Enter the certification request retry number. The retry number must be between 1 and 100.
		Set to Default	Select this option to set the default retry period to 1 minute.
	CRL Optional	Action	Select **Enable** to bypass the Certificate Revocation List. If you select **Disable**, Certificate Revocation list is checked.
	Certificate Query	Action	Select an option to enable, disable or make no change to certificate query. • If you select **Enable**, certificate query will be added to all trust points on the router. • If you select **Disable**, the certificate will not be queried.
	RSA Key pairs	Action	Select an option to generate, delete or make no change to the RSA key pairs. This feature allows you to configure a Cisco IOS router to have multiple key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.
		Key Type	Specify the key type: • General Purpose—To generate a general purpose key pair that is used for both encryption and signature. • Usage—To generate separate usage key pairs for encrypting and signing documents.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the numeric `56` or `K`*n*, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`.

Crypto Map Task

You can use the Crypto Map Server system-define task to configure IPSec on devices.

Note You must configure the IKE configuration system-defined task (see Internet Key Exchange (IKE) Configuration Task) and Transform system-defined task (see Transform System-Defined Task) before configuring the Crypto Map system-defined task.

The following device categories are supported by this task:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the Crypto Map Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Crypto Map Configuration dialog box are:

Group	Sub-Group	Field	Descriptions
IOS Parameters	Configuration	Action	Select an option to add, remove, or make no change to the IOS configuration.
		Map Name	Enter the name for the Crypto Map.
		Map Number	Enter the number for the Crypto Map. The value must be between 1-65535.
		Map Type	Select the map type (manual or isakmp) for the Crypto Map.
		Map Description	Enter the description for the Crypto Map.
		Crypto ACL	Enter the extended access list for Crypto Map.
		IPSec Peer	Enter the IPSec peer to be associated with the Crypto Map.
		Transform Set name	Enter the transform set name to be used with the Crypto Map.
PIX Parameters	Configuration	Action	Select an option to add, remove, or make no change to the PIX configuration.
		Map Name	Enter the name for the Crypto Map.
		Map Number	Enter the number for the Crypto Map. Value must be between 1-65535.
		Map Type	Select the type (manual or isakmp) for the Crypto Map.
		Crypto ACL	Enter the extended access list for Crypto Map.
		IPSec Peer	Enter the IPSec peer to be associated with the Crypto Map.
		Transform Set name	Enter the transform set name to be used with the Crypto Map.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

DNS Task

You can use the DNS system-defined task to configure DNS (Domain Name Server) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the DNS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the DNS Configuration dialog box are:

Group	**Sub-Group**	**Field**	**Description**
Common Parameters	DNS Server	Add	Enter the IP address(es) of DNS name server(s) that you want to add. Separate multiple addresses with commas. If the device accepts only one DNS server, then the first address will be considered.
		Remove	Enter the IP address(es) of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
	Domain Name	Name	Enter the domain name(s) to complete unqualified hostnames. If a device has a domain list enabled, it will be used to complete unqualified hostnames instead of the domain name. Separate multiple addresses with commas. If the device accepts only one domain name, then the first entry will be considered.
		Remove	Select this option to remove the domain names.
IOS Parameters		Domain Lookup	Select to enable or disable IP DNS-based hostname-to-address translation.
		CLNS NSAP	Select to enable or disable or make no change to the CLNS NSAP option. If this option is enabled, any packet with the specified CLNS NSAP prefix causes CLNS (Connectionless Network Service) protocol to behave as if no route were found.
		OSPF	Select to enable or disable or make no change to the OSPF (Open Shortest Path First) protocol option.
	Domain List	Action	Select an option to add, remove, or make no change to the domain list.

Group	Sub-Group	Field	Description
		Domain List	Enter domain names to complete unqualified hostnames, or add to the existing list. Separate multiple domain names with commas. Do not include an initial period before domain names.
CatOS Parameters		1st Server Primary	Select to make DNS name server entered in Add field, the default or the primary name server.
		Domain Lookup	Select an option to enable, disable, or make no change to the domain lookup.
Content Engine Parameters		Serial Lookup	Select an option to enable, disable, or make no change to the serial lookup.
CSS Parameters	Secondary DNS Server	Add (Hostname or IP Address)	Enter the hostname or an IP address of a secondary server, that you want to add. A maximum of two IP addresses are allowed. The order in which you enter them is the order in which they are used if the primary DNS server fails. Separate multiple addresses with a comma.
		Remove (Hostname or IP Address)	Enter a hostname or an IP address of a secondary server, that you want to remove. A maximum of two IP addresses are allowed. Separate multiple addresses with a comma
NAM Parameters		Disable Nameservers	Select to disable domain name servers.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Enable Password Task

You can use the Enable Password system-defined, configuration task to change the enable and secret passwords, which allow users to enter the enable mode on devices.

When you enable or disable an enable password, the change is made on the device and in Device and Credential Repository.

Note If you disable the enable password on a device, you cannot enter the enable mode on that device unless you previously enabled an alternative type of enable mode authentication.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the Enable Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note If you change the enable password on a Catalyst device with an RSM module using this task, the RSM enable password is also changed.

The fields in the Enable Password Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Setup	Action	Select an option to enable, disable or make no change to the enable password.
		Password	Enter the enable password.
		Verify	Re-enter the password.
IOS Parameters	Password	Level (1-15)	Set the Enable Password level. The level can be between 1 and 15. 15 is the default level. For an IOS device, it is not advised to disable both Enable Password and Enable Secret password. This is because the IOS device will not allow you to go into the Enable mode of the device. You can do this only if you have the console password for the device. If you have selected Enable Password as **No Change** in the Common Parameters pane, and selected Disable for Enable Secret in the IOS Parameters pane, then Enable Secret Password is updated in the Device and Credentials database. If you have selected Enable Password as **Disable** in the Common Parameters pane, and selected **No Change** for Enable Secret in the IOS Parameters pane, then Enable Password is updated in the Device and Credentials database.
		Encrypted	Select this option to encrypt the password.
		Update RME Credentials	Select this to update RME credentials. For details see Understanding the NetConfig Credentials Configuration Tasks
	Secret	Action	Select an option to enable, disable or make no change to the secret password.s
		Secret	Enter the secret password.
		Verify	Re-enter the password.
		Level (1-15)	Set the password level. The level can be between 1 and 15. 15 is the default level.

Group	Sub-group	Field	Description
		Encrypted	Select this option to encrypt the password.
CatOS Parameters	Password	Apply Command on Modules	Select to apply the command on the modules. If you have selected **Disable** as the action in the Common Parameters group, then the password will be removed.
PIX Parameters		Level(0-15)	Set the password level. The level can be between 0 and 15. 15 is the default level.
		Encrypted (Password should be 16 characters)	Select this option if the password you are entering is already encrypted. If you select this option ensure that your password is 16 characters.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

HTTP Server Task

You can use HTTP Sever to configure HTTP access on IOS devices which have been configured for VPN functionality.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS

For more details, see Table 9-3.

You can enter the details of this task in the HTTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the HTTP Server Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Server	Action	Select an option to enable, disable or make no change to the HTTP access on the device.
	Port	Number [0-65535]	Specify the HTTP server port number.
		Set to Default	Select this option to set the default port (80).
IOS Parameters	Authentication	Action	Select an option to enable, disable or make no change to the authentication method.

Group	Sub-group	Field	Description
		Method	Select an authentication method: • aaa • enable • local • tacacs
	Access List	Action	Select an option to enable, disable or make no change to the access list.
		ACL Number/Name	Enter the Access Control List number or name to be used. The access list number must be between 1 to 99.
CatOS Parameters			No category-specific commands.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

You will lose Telnet access to the device if you configure HTTP Server. The Device may require TACACS/RADIUS/Local username and password after configuring HTTP Server. You should make sure that the device has the appropriate login configured. The username and password has to be stored in the RME Database.

IOS Devices with VPN Images

You can determine VPN images from the naming convention used for IOS images. The naming convention follows *xxxx-yyyy-ww* format.

Where, *xxxx* represents platform, *yyyy* represents features and ww represents format. If the middle value (*yyyy*) contains, the numeric `56` or `K`*n*, where *n* is a number between 1 and 9, then this is a VPN image.

For example, `C7100-IS56I-M` is a VPN image, since it contains the number `56`

Local Username Task

You can use the Local Username system-defined task configure local username and password authentication on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- CSS

For more details, see Table 9-3.

You can enter the details of this task in the Local Username Task Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Local Username Task Configuration dialog box are:

Group	Sub-Group	Field	Description
Common Parameters	Local User Setup	Action	Select an option to add, remove or make no change to the local username setup.
		Username	Enter the local username.
		Password	Enter local username password.
		Verify	Re-enter the password.
IOS Parameters	Local User Setup	Privilege Level [0-15]	Set the required privilege level.
Local User Setup		Privilege Level [0-15]	Set the required privilege level.
		No HangUp	Select this option to enable No Hang Up mode.
		No Escape	Select this option to enable No Escape mode.
Local User Login Authentication		Action	Select to enable, disable or make no change to the local user authentication group of fields.
	Local Username Credentials (Update RME creds)	Username	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Password	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
CSS Parameters			For CSS devices: • The username length should be between 1 and 16 characters. • The local password length be between 6 and 16 characters. • The DES-Encrypted password length should be between 6 and 64 characters.
Local User Setup		SuperUser	Select this option to designate the local user as superuser.
		Password Type	Select the password type from these options: • Local • Encrypted • DES_Encrypted
Directory Access		Configure Directory Access	Select this option if you want to configure directory access. Defines the CSS directory access levels. By default, CSS assigns users with read and write access to the directories. Changing the access level also affects the use of the CLI commands associated with the directories.

Group	Sub-Group	Field	Description
	Directories	Script	Select the required access option to the Script directory: • No Access • Read And Write • Read • Write
		Log	Select the required access option to the Log directory: • No Access • Read And Write • Read • Write
		Root	Select the required access option to the Root directory: • No Access • Read And Write • Read • Write
		Archive	Select the required access option to the Archive directory: • No Access • Read And Write • Read • Write
		Release Root	Select the required access option to the Release Root directory: • No Access • Read And Write • Read • Write
		Core	Select the required access option to the Core directory: • No Access • Read And Write • Read • Write
		MIB	Select the required access option to the MIB directory: • No Access • Read And Write • Read • Write

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

IGMP Configuration Task

You can use this task to configure the Internet Group Management Protocol (IGMP) on a cable interface.

Note You can apply this task only on a single IOS device at a time. For details, see Table 9-3.

You can enter the details of this task in the IGMP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the IGMP Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters			
IGMP Configuration	Interface	Interfaces	Select the required option to specify the interface to be configured for IGMP, or to make no change to the existing interface selection: • Not Selected • FastEthernet0/0 • FastEthernet0/ • Cable1/0
		Action	Select the required option to enable, disable, or make no change to the Interface sub-group of fields.
		PIM Mode	Select the required PIM mode option. Select No Change to retain any previous mode selection: • No Change • dense-mode • sparse-mode • sparse-dense-mode
IGMP Parameters		Action	Select the required option to replace the values in, or to make no change to the IGMP Parameters group of fields.
		IGMP Version	Select the required IGMP version from the supported versions: • 1 • 2 • 3

Group	Sub-group	Field	Description
		Last Memory Query Interval [100-25500 in msec]	Enter the time interval between the IGMP specific messages sent by the router. Enter the last memory query interval in seconds. You can enter an interval between 100—25500 milliseconds. The default is 1000 milliseconds.
		Query Maximum Response Time[1-25 in sec]	Enter the maximum response time advertised in the IGMP queries. This option is enabled when IGMP version 2 is configured. You can enter a response time between 1—25 seconds. The default is 10 seconds.
		Query Interval [1-65535 in sec]	Indicates a time interval when the Cisco IOS software sends IGMP host queries. Enter a query interval between 1—65535 seconds. The default is 60 seconds.
		Query Timeout [60-300 in sec]	Indicates the timeout period when the router takes over as a querier of an interface after the previous querier stopped querying. You can enter a value between 60—300 seconds. The default is 2* Query Interval second.
		Helper Address (Should be in IP address format)	Indicates the IP address that will receive all IGMP host reports and where you can leave messages. This option is enabled when IGMP version 2 is configured. Enter the Helper Address in the IP Address format.
Group Configuration		Action	Select the required option to add values to, or to make no change to the Group Configuration group of fields.
		ACL to control joining of Multicast Group	Allows you to control the multicast groups. You can enter either the IP access list name or number. The valid range is between 1 - 99.
		Join Group Multicast Address (multiple addresses should be separated by commas)	Adds Join Group Multicast Address to the Multicast Address table. Enter the addresses, separated by commas.
		Static Group Multicast Address (multiple addresses should be separated by comma)	Adds Static Group Multicast Address to the Multicast Address table. Enter the addresses, separated by commas.
		Populate for all Groups	Allows you to apply the configuration to all groups.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

For more information regarding the IP addresses and IP multicast addresses refer to:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca75b.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca76d.html

Interface IP Address Configuration Task

You can use this task to configure the IP address of a cable interface.

Note You can apply this task only on a single IOS device at a time. For details, see Table 9-3.

You can enter the details of this task in the Interface IP Address Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Interface IP Address Configuration dialog box are:

Group	Sub-group	Field	Description
Cable Parameters			
Interface IP Configuration		Cable Interface	Select the required cable interface for configuring the IP address, or select **Not Selected** to make no change to any previous selection: • Not Selected • FastEthernet0/0 • FastEthernet0/1 • Cable1/0
		Action	Select the required action: • No Change—Makes no change to the IP Addresses • Replace—Replaces the IP Addresses • Remove Primary—Removes the primary IP Address. • Remove Secondary—Removes the secondary IP Address. • Remove All—Removes both primary and secondary IP Addresses.
	IPAddress	Primary	Enter the primary IP address.
		Secondary	Enter the secondary IP address.
	Subnet Mask	Primary	Enter the primary subnet mask.
		Secondary	Enter the secondary subnet mask.

Note The values for interfaces are as returned by device.

Click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Internet Key Exchange (IKE) Configuration Task

Use the Internet Key Exchange (IKE) Configuration System task to configure IPSec on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the IKE Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	**Sub-group**	**Field**	**Description**
IOS Parameters			
ISAKMP		Action	Select to enable, disable, or make no change to ISAKMP.
ISAKMP Policy	ISAKMP Policy Priority	Action	Select to add, remove, or make no change to ISAKMP policy priority.
		Priority [1-10000]	Enter the policy priority number Value must be between 1—10000.
	Encryption	Action	Select to enable, disable, or make no change to encryption type.
		Type	Select the type of encryption for the policy: • 3des • des
	Hash	Action	Select to enable, disable, or make no change to the hash algorithm.
		Algorithm	Select the type of hash algorithm: • sha • md5
	Authentication	Action	Select to enable, disable, or make no change to the authentication method.
		Method	Select the type of authentication method: • rsa-sig • rsa-encr • pre-share
	Group	Action	Select to enable, disable, or make no change to the Diffie-Hellman group identifier group.
		Value	Enter the Diffie-Hellman group identifier. Value must be 1 or 2.
	Lifetime	Action	Select to enable, disable, or make no change to the lifetime value.
		Seconds [60-86400]	Enter the lifetime value in seconds. Value must be between 60—86400 seconds.

Group	Sub-group	Field	Description
PIX Parameters			
ISAKMP		Action	Select to enable, disable, or make no change to ISAKMP.
		Interface	Select the interface: • Inside • Outside
ISAKMP Policy	ISAKMP Policy Priority	Action	Select to add, remove, or make no change to ISAKMP policy priority.
		Priority [1-65534]	Enter the policy priority number Value must be between 1—10000.
	Encryption	Action	Select to enable, disable, or make no change to encryption type.
		Type:	Select the type of encryption: • aes • aes-192 • aes-256 • des • 3des
	Hash	Action	Select to enable, disable, or make no change to the hash algorithm.
		Algorithm	Select type of hash algorithm: • sha • md5
	Authentication	Action	Select to enable, disable, or make no change to the authentication method.
		Method	Select the type of authentication method: • rsa-sig • pre-share
	Group	Action	Select to enable, disable, or make no change to the Diffie-Hellman group identifier group.
		Value	Enter the Diffie-Hellman group identifier. Value must be 1, 2 or 5.
	Lifetime	Action	Select to enable, disable, or make no change to the lifetime value.
		Seconds [120-86400]	Enter the lifetime in seconds. Value must be between 120—86400 seconds.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

NTP Server Configuration Task

You can use the NTP Server system-defined task to configure Network Time Protocol (NTP) on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- CSS
- CE

For more details, see Table 9-3.

You can enter the details of this task in the NTP Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters	NTP Server	Action	Select to add, remove, or make no change to Network Time Protocol.
		Host Name/IP Address	Enter IP address of NTP server to which devices will send time-of day requests.
IOS Parameters	NTP Server	Server Type	Select the required server type.
		Version	Select the server version.
		Server Key (0-4294967295)	Enter the NTP server Key. The value must be between 0—4294967295.
		Verify Server Key	Re-enter the Key to confirm.
		Source Interface (Interface Name)	Enter the source interface name.
		Preferred	Select an option to specify whether it is a preferred interface.
	NTP Authentication Key	Action	Select to add, remove, or make no change to the NTP authentication Key.
		Number [1 to 4294967295]	Enter the number of Key bits. The value must be between 1 to 4294967295 Key bits.
		Verify Number	Re-enter the number to confirm.
		MD5 Number (Max 8 chars)	Enter the MD5 number. It should be a maximum of 8 characters.
	NTP Authentication	NTP Authentication	Select to enable, disable, or make no change to NTP authentication.
	NTP Calendar	Action	Select to add, remove, or make no change to the NTP calendar.
	NTP Access Group	Action	Select to add, remove, or make no change to the NTP access group.

Group	Sub-group	Field	Description
		Access Type	Select the required action type: • QueryOnly • ServeOnly • Serve • Peer
		ACL Number [1-99]	Enter the ACL number. It should be a value between 1 and 99.
	NTP Trusted Key	Action	Select to add, remove, or make no change to the NTP trusted Key.
		Key Number [1-4294967295]	Enter the Key number. It must be a value between 1—4294967295.
		Verify Key Number	Re-enter the Key number to verify.
CatOS Parameters	NTP Server	Server Key [Range:1 to 4292945295]	Enter the NTP server Key. The value must be between 1 to 4292945295.
		Verify Server Key	Re-enter the Key to confirm.
	NTP Client	Client Action	Select to enable, disable, or make no change to NTP client.
	NTP Authentication	NTP Authentication	Select to enable, disable, or make no change to NTP authentication.
	NTP Key	Action	Select to add, remove, or make no change to the NTP Key.
		Key Number [1 to 4292945295]	Enter the NTP server Key. The value must be between 1 to 4292945295.
		Verify Key Number	Re-enter the Key to confirm.
		Type	Select the required Key type.
		MD5 Number [Max 32 chars]	Enter the MD5 number. It should be a maximum of 32 characters.
CE Parameters	NTP Server	Action	Select to enable, disable, or make no change to the NTP server.
		Server Type	Select the required server type.
CSS Parameters		NTP Server Version	Select the required NTP server version.
	NTP Server Poll Interval	Action	Select to add, remove, or make no change to the NTP poll interval.
		Poll Interval [16-16284 seconds]	Specify the poll interval. The value must be between 16—16284 seconds.

RADIUS Server Configuration Task

You can you use the RADIUS system-defined task to configure RADIUS on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)

- CSS
- CE

For more details, see Table 9-3.

You can enter the details of this task in the RADUIS Server Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
Host Configuration		Action	Select to enable, disable, or make no change to the server configuration.
		Server Name	Enter the server name.
		Auth Port (0-65536)	Enter port used for authentication by RADIUS server.
Key Configuration		Action	Select to enable, disable, or make no change to the key configuration.
		Key	Enter RADIUS authentication and encryption key string used by server specified in Host area.
		Verify	Re-enter RADIUS key.
Login Authentication		Action	Select to enable, disable, or make no change to the login authentication. This is not applicable for CSS
	RADIUS Credentials (Update RME creds)	Username	Enter the username. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
		Password	Enter the password. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
		Verify	Re-enter the password to verify. For details see Understanding the NetConfig Credentials Configuration Tasks. In case of CSS devices, this value will be used to update the Primary login details.
IOS Parameters			
Login Authentication	List	Name	Enter default or named list.
		Set to Default	Select the set the default list.

Group	Sub-group	Field	Description
	Type	Options (Drop-down list 1)	Select the required option; • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.
New Model		Action	Select to enable, disable, or make no change to new model state.
Enable mode Authentication		Action	Select to add, remove, or make no change to the enable mode authentication.
	Credentials	Username	Enter the enable username.
		Password	Enter the enable password.
		Verify	Re-enter the enable password.
	Type	Options (Drop-down list 1)	Select the required option: • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.
Content Engine Parameters			No category-specific commands.
CSS Parameters	Host Configuration	Action	Select to enable, disable, or make no change to the host configuration.
		Secondary Server Name (Host Name or IP Address)	Enter the secondary server hostname or IP address.
		Secondary Server Key	Enter the key for the secondary server. Defines the secret string for authentication transactions between the RADIUS server and the CSS. Enter a case-sensitive string with a maximum of 16 characters.
		Verify	Re-enter the key to verify.

Group	Sub-group	Field	Description
		Authentication Port (1-65535)	Enter custom authentication port of RADIUS server. Value must be between 0-65535. Optional field. Defines the UDP port on the secondary RADIUS server that receives authentication packets from clients. Enter a number from 0 to 65535. The default is 1645.
Other Parameters		Dead Time in seconds (1-255)	Enter the dead time in seconds. the value must be between 0—255. Enter a number from 0 to 255. The default is 5. If you enter 0, the dead time is disabled and the CSS does not send probe access-request packets to the non-responsive server. This command applies to primary and secondary servers.
		Remove	Select to remove the dead time specification. Use the **no** form of this command to reset the dead-time period to its default of 5 seconds.
		Retransmit (1-30)	Enter the retransmit value (between 1—30). Number of times that the CSS retransmits an authentication request. Enter a number from 1 to 30. The default number is 3.
		Remove	Use the **no** form of this command to reset the retransmission of authentication request to its default of 3.
		Source Interface Host (Host Name or IP Address)	Enter the source interface hostname or IP address. Source Interface Host configuration is required to accept authentication from the RADIUS client. Note that this IP interface address is used for the NAS-IP-Address RADIUS attribute in the RADIUS Authentication Request.
		Remove	Select to remove the source interface specification.
		Timeout (1-255):	Enter the timeout value (between 1—2555). Timeout specifies the interval that the CSS waits for a reply to a RADIUS request before retransmitting requests to the RADIUS server.
		Remove	Select the remove option to reset the interval to its default of 10 seconds.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

RCP Configuration Task

You can use the RCP system-defined configuration task to configure rcp on devices.

This task supports the IOS category of device including Cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the RCP Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box)

The fields in the RCP Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters	Enable	Action	Select to enable or disable rcp state. To make rcp setup changes without enabling or disabling rcp, select **No Change**.
	RCP User Setup	Action	Select the required option to add to, or to remove current user from rcp authentication list. To make rcp setup changes without enabling or disabling rcp, select **No Change**.
		Local Username	Enter local name of user whose rcp access you are modifying.
		Remote Host	Enter IP address of remote host from which local device will accept remotely executed commands.
		Remote Username	Enter username on remote host from which device will accept remote commands.
		Enable Mode Commands	Click to allow remote user to run enable commands using rsh or to copy files to device using rcp.
		add/remove	Click add to add current user to rcp authentication list. Click remove to remove current user from rcp authentication list.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Reload Task

You can use the Reload task to schedule reload of devices. This task supports the IOS, Cat OS, SFS, NAM, CE, FastSwitch, PIX, CSS and Cable categories of devices. For more details, see Table 9-3.

You can enter the details of this task in the Reload Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box)

The fields in the Reload Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
CatOS Parameters			No category-specific parameters.

CE Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
NAM Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.
SFS Parameters			No category-specific parameters.
Fast Switch parameters			No category-specific parameters.
PIX Parameters			No category-specific parameters.
CSS Parameters			No category-specific parameters.
Cable Parameters	Do not Save config before reload	Action	You can: • Check this option if you do not want to save the configurations before reloading. or • Uncheck this option if you want to save the configurations before reloading.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which the reload task applies.

SNMP Community Configuration Task

You can use the SNMP Community Configuration system-defined task to replace, add, and remove device SNMP community strings.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the SNMP Community Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Community Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Read-only	Action	Select an option to replace, add, remove, or make no change to a read-only SNMP community string. • If you select **Replace**, the new community string replaces the corresponding community string in the Device and Credential Repository (DCR). This action also deletes the current SNMP credentials on the device. • If you select the **Add** or **Remove** option, the new SNMP community strings are configured in the device alone and DCR is untouched. However if you select **Replace**, then the new SNMP community strings replace the community strings in the device as well as in DCR. If you select **No Change**, no change will be made to the Read-only Community string.
		Community String	Enter the community string.
		Verify	Re-enter the community string.
	Read-write	Action	Select an option to replace, add, remove, or make no change to a read-write SNMP community string. • If you select **Replace**, the new community string replaces the corresponding community string in the Device and Credential Repository. • If you select **Add** or **Remove**, the new SNMP community strings are configured in the device alone and DCR is untouched. However if you select **Replace**, then the new SNMP community strings replace the community strings in the device as well as in DCR. If you select **No Change**, no change will be made to the Read-write Community string.
		Community String	Enter the community string.
		Verify	Re-enter the community string.
IOS Parameters	Setup View (Optional)	MIB View (Optional)	Enter name of a previously defined view that defines objects available to community. Optional field.
		OID -Tree	Indicates the Object Identifier of ASN.1 subtree to include or exclude from the view. To identify an Object Identifier ASN.1 subtree, enter a numerical string such as 1.3.6.2.4 or a word such as system. To identify a subtree family, enter a wildcard, an asterisk (*), such as 1.3.*.4. Enter the MIB OID-Tree name.

Group	Sub-group	Field	Description
		Type	Include or exclude all the objects specified in the MIB OID subtree you identified in the previous field. Select Included or Excluded from the drop down list.
	Access List (Optional)	Access List (Optional)	Enter integer from 1 to 99 to specify a named or numbered access list of IP addresses allowed to use the community string to access SNMP agent. Optional field.
CatOS Parameters			No category-specific parameters.
CE Parameters			No category-specific parameters.
PIX Parameters			No category-specific parameters.
CSS Parameters			No category-specific parameters.
NAM Parameters			No category-specific parameters.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

SNMP Security Configuration Task

You can use this task to configure SNMP Security feature on the following device categories:

- IOS (including Cable devices)
- Content Engine

For more details, see Table 9-3.

You can enter the details of this task in the SNMP Security Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Security Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters		Action	Select an option, to add, remove, or make no change to the common parameters.
		(Drop-down list)	Select the required option for SNMP Groups/Users: • Group & Users • Group • Users When you select the Group option while adding task instances for this task, the user fields will not be disabled. This is because NetConfig needs the user information for configuring SNMP group commands in Catalyst OS devices.
		Group Name	Enter the group name. Indicates the SNMP Group in the SNMP protocol context.
		SNMP Versions	Select the SNMP version. SNMP version 1 and version 2 have No Auth and No Privacy. Version 3 has all levels of security.
	Users * - The entries in the first row will be updated in Device and Credential Repository	User Names Authen Pswds Authen Algorithm Privacy Paswds	• Username—Indicates the name of the user in the SNMPv3 protocol. • Authenticating Passwords—Indicates that the user is part of the group that is assigned Auth No Privacy or Auth Privacy security level. • Authenticating Algorithm—Indicates the authenticating algorithm is assigned to a group with Auth No Privacy or Auth Privacy security levels. • Privacy passwords—Indicates user is part of a group assigned Auth Privacy level of security. You can specify up to five usernames, enter authentication passwords, select the authentication algorithm and specify the privacy passwords.
	Config Access Control [optional]		This section allows you to configure access options for an SNMP group.
		Read View	Specify the read view. This view can be viewed by users assigned to a specified group. Indicates an alphanumeric label, not exceeding 64 characters, for the SNMP view entry you are creating or updating.
		Write View	Specify the write view. Allows all users in the specified group to add, modify, or create a configuration.
		Notify View	Specify the notify view. This view notifies all the users in the specified group.
IOS Parameters	Access Control (optional)	Access List [1-99]	Enter the number of an Access List (1—99).

Group	Sub-group	Field	Description
	Engine ID [optional]	Action	Select to add, remove, or make no change to the engine configuration. SNMP Engine ID is an identification name for the local or remote SNMP engine.
		Type	Select the type of engine: • Local—Local SNMP server engine. • Remote—Remote SNMP server engine.
		ID	Enter the Engine ID (identification name for the local or remote SNMP engine). MIB OID Tree- Indicates the Object Identifier of ASN.1 subtree to include or exclude from the view. To identify an Object Identifier ASN.1 subtree, enter a numerical string such as 1.3.6.2.4 or a word such as system. To identify a subtree family, enter a wildcard, an asterisk (*), such as 1.3.*.4.
		Remote host	Enter the hostname or IP address of the remote SNMP entity to which the user belongs.
Content Engine Parameters		Remote Engine ID [Optional]	Enter the remote engine ID (identification name). This is an optional field.

The SNMP Security template enables you to configure Groups as well as Users with certain privileges. These Groups can be rolled back but the Users cannot be rolled back.

This is because the User details will not be available in the running configuration. Since NetConfig uses the running config to do roll back, rolling back Users is not possible.You should run a separate job to remove or add Users as required.

For each device category, click on **Applicable Devices** to view the devices in your selection.

- For more information on how to configure SNMP, refer to: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66b.html

SNMP Traps Configuration Task

You can use this task to configure the host, trap notification, and trap/inform parameters. You can specify security parameters to communicate securely with the SNMP host. See SNMP Security Configuration Task to configure the SNMP security.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- CSS
- NAM

For more details, see Table 9-3.

You can enter the details of this task in the SNMP Traps Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the SNMP Traps Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Traps Notification	Action	Select to enable, disable, or make no change to the traps notification configuration. If you select **Enable**, the server will receive SNMP traps. If you select **Disable** the server will not receive any SNMP traps.
IOS Parameters			
Traps Notification Options	Type	Environmental	Select this to send only environmental traps to the host.
		SNMP	Select this to send the SNMP traps to the host.
Host Configuration		Action	Select to add, remove, or make no change to the host configuration.
		Username	Specific the user name that is used for authentication. This field is available when No Authentication, Authentication or Privacy are selected.
		Host	Enter the hostname or IP address.
		SNMP Security	Select the SNMP security method: • SecureV2c • NoAuthenticationV3 • AuthenticationV3 • PrivacyV3 • None
		Notification Type	Select the notification type: • Trap • Inform
		UDP Port [0-65535]	Indicates the port that will receive the SNMP requests. The range for a valid port number between 0—65535. The default is 162.
	Community String	String	Enter the community string.
		Verify	Re-enter the community string to confirm.
	Direct Traps To Host	Environmental	Select this to send only environmental traps to the host.
		SNMP	Select this to send the SNMP traps to the host.
Trap/Inform Configuration	Traps Message	Action	Select to change, replace, disable or make no change to the trap configuration.

Group	Sub-group	Field	Description
		Trap Timeout [1-1000 s]:	Specify the trap timeout value. This must be between 1—1000 seconds.
		Trap Queue Length [1-1000 events]:	Specify the trap queue length. the number of events that you specify must be between 1—1000.
	Inform Request	Action	Select to replace, disable, or make no change to the inform request.
		Inform Retries [0-100]	Enter the inform retires. The value should be between 0—100.
		Inform Timeout [0-4294967295]	Specify the inform timeout value. This must be between 0—4294967295.
		Inform Pending [0-4294967295]	Specify the inform pending value. This must be between 0—4294967295.
CatOS Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Enter the hostname or IP address.
		Community String	Enter the community string.
		Verify	Re-enter the community string to confirm.
ContentEngine Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Enter the hostname or IP address.
		Community String	Enter the community string.
		Verify	Re-enter the community string to confirm.
		SNMP Security	Select the SNMP security method.
PIX Parameters	Host Configuration	Action	Select to add, remove, or make no change to the host configuration.
		Host	Specify an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come. You can specify up to five SNMP management stations.
		Interface	Select the interface: • Inside [default] • Outside

Group	Sub-group	Field	Description
		Notification Type	Select the notification type: • Trap & Poll [default]—Allows both traps and polls to be acted upon. • Trap—Only traps will be sent. This host will not be allowed to poll. • Poll—Traps will not be sent. This host will be allowed to poll.
CSS Parameters		Action	Select to add, remove, or make no change to the parameters such as host name or IP address, trap community, source IP address in traps, specific host, trap type, event, etc.
		Host Name or IP Address	Enter the hostname or IP address of an SNMP host that has been configured to receive traps. A maximum of 5 hosts can be configured.
		Trap Community	Enter the trap community string/name to use when sending traps to the specified SNMP host. Enter an unquoted text string with no spaces and a maximum length of 12 characters.
		Verify	Re-enter the trap community string to confirm.
		Source IP Address in Traps	Select the source IP address in traps. To set the source IP address in the traps generated by CSS select one of these options: • Egress Port—Obtains the source IP address for the SNMP traps from the VLAN circuit IP address configured on the egress port used to send the trap. You do not need to enter an IP address because the address is determined dynamically by the CSS. • Management—Places the management port IP address in the source IP field of the trap. This is the default setting. • Specific Host—Allows the user to enter the IP address to be used in the, source IP field of the traps. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) in the Specific Host field (the next field). • No Change (No change will be made to the source IP address if you select this option.)
		Specific Host	In the previous field, that is, Source IP Address in Traps, if you have selected the Specific Host option, then specify the IP Address of the specific host in this field.

Group	Sub-group	Field	Description
		Trap Type	Select the trap type: • No Change (No change will be made to the trap type if you select this option). • Enterprise—When you use this keyword alone, it enables enterprise traps. You must enable enterprise traps before you configure an enterprise trap option. • Generic—The generic SNMP traps consist of cold start, warm start, link down, and link up.
		Event	Select the event: • None • Module Transition • Power Supply Transition • Illegal Packet DOS attack • LAND DOS attack • Smurf DOS attack • SYN DOS attack • Lifetick message failure • Login Failure • System reload • Reporter state transitions • Service transition
NAM Syslog Host Configuration Parameters		Action	Select to add, remove, or make no change to the syslog host configuration.
		Index[1-65535]	Enter the syslog host index. The value should be between 1—65535.
		Host IP Address	Enter the host name or IP address.
		Community String	Enter the community string.
		Verify	Verify the community string.
		UDP Port[1-65535]	Enter the UDP port. The value should be between 1—65535.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

For more information regarding configuring SNMP, refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66b.html

Syslog Task

You can use the Syslog system-defined task to configure the collection of syslog messages from devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS
- NAM
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the Syslog Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Syslog Configuration dialog box are:

Group	Sub-group	Field	Description
Common Parameters	Logging Host	Action	Select the required option to enable, disable, or make no change to list of hosts that receive syslog messages.
		Ex: host1.domain,host2,1.2.3.4:	Enter IP address of hosts to add or remove from list of hosts that receive syslog messages. Separate multiple addresses with commas.
IOS Parameters			
Logging On		Action	Select the required option to enable, disable, or make no change to syslog state. Select No Change to make syslog setup changes without enabling or disabling syslog logging.
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which to log syslog messages.
Logging Level	Buffered	Action	Select the required option to enable, disable, or make no change to the buffered logging level.

Group	Sub-group	Field	Description
		Conditions	Select the required logging level from the drop-down list: • Default • alerts • critical • debugging • emergencies • errors • informational • notifications • warnings
	Console	Action	Select the required option to enable, disable, or make no change to the console logging level.
		Conditions	Select the required logging level from the drop-down list.
	Monitor	Action	Select the required option to enable, disable, or make no change to the monitor logging level.
		Conditions	Select the required logging level from the drop-down list.
	Trap	Action	Select the required option to enable, disable, or make no change to the trap logging level.
		Conditions	Select the required logging level from the drop-down list.
CatOS Parameters			
Console Logging On		Action	Select the required option to enable, disable, or make no change to console logging.
Server Logging On		Action	Select the required option to enable, disable, or make no change to server logging.
Logging Level		Action	Select the required option to enable, disable, or make no change to the logging level.
		Facility	Select the logging facility to which to log syslog messages.
		Level	Select the required logging level from the drop-down list.
Content Engine Parameters			
Logging On		Action	Select the required option to enable, disable, or make no change to logging.
Destination		Console	Select this option to specify the console as the logging destination.
		Disk	Select this option to specify the disk as the logging destination.
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which to log syslog messages.
Logging Priority	Console	Action	Select the required option to enable, disable, or make no change to the console logging priority.

Group	Sub-group	Field	Description
		Conditions	Select the required logging priority from the drop-down list.
	Disk	Action	Select the required option to enable, disable, or make no change to the disk logging priority.
		Conditions	Select the required logging priority from the drop-down list.
	Host	Action	Select the required option to enable, disable, or make no change to the host logging priority.
		Conditions	Select the required logging priority from the drop-down list.
PIX Parameters		Time Stamp	Select the required option to enable, disable, or make no change to the time stamp specification.
		Logging On	
Logging Facility		Action	Select the required option to enable, disable, or make no change to syslog logging facility.
		Parameter	Select the logging facility to which to log syslog messages.
Message		Action	Select the required option to enable, disable, or make no change to the syslog message configuration.
		Syslog Message ID	Enter the syslog message ID.
		Conditions	Select the required logging level from the drop-down list.
Logging Level	Buffered	Clear Buffer	Select to clear the buffer.
		Action	Select the required option to enable, disable, or make no change to the buffered logging level.
		Conditions	Select the required logging level from the drop-down list.
	Console	Action	Select the required option to enable, disable, or make no change to the console logging level.
		Conditions	Select the required logging level from the drop-down list.
	Monitor	Action	Select the required option to enable, disable, or make no change to the monitor logging level.
		Conditions	Select the required logging level from the drop-down list.
	Trap	Action	Select the required option to enable, disable, or make no change to the trap logging level.
		Conditions	Select the required logging level from the drop-down list.
CSS Parameters		Facility	Select the logging facility to which to log syslog messages.
		Logging Level	Select the required logging level from the drop-down list.
		CLI Command	Select the required option to add, remove, or make no change to the CLI commands.
	Logging to Disk	Disk	Select the required option to add, remove, or make no change to logging to disk.
		Logfile Name	Enter the log file name.
		Buffer	Select the required option to add, remove, or make no change to the buffer configuration.

Group	Sub-group	Field	Description
		Size [0-64000]	Enter the size of the buffer. Enter a value between 0—64000 bytes.
		To sys.log	Select the required option to add, remove, or make no change to the option to log to a file called sys.log.
	Logging to Line	Line	Choose this option to send the log activity of a subsystem to an active CSS session.
		Active Session Name	Enter the name of the active session. Enter a case-sensitive unquoted text string with a maximum length of 32 characters.
	Logging to Mail	Send Mail	Select the required option to add, remove, or make no change to the e-mail option.
		Mail Address	Enter the e-mail IDs (comma separated).
		SMTP Host (Name or IP Address)	Enter the SMTP hostname or the IP address.
		Logging Level	Select the required logging level from the drop-down list.
		Domain Name (Optional)	Enter the domain name of the SMTP host. This is an optional field.
NAM Parameters	MIB Threshold	Local	Select the required option to enable, disable, or make no change to the local MIB threshold.
		Remote	Select the required option to enable, disable, or make no change to the remote MIB threshold.
	Voice	Local	Select the required option to enable, disable, or make no change to the voice (local).
		Remote	Select the required option to enable, disable, or make no change to the voice (remote).
	System	Local	Select the required option to enable, disable, or make no change to system (local).
		Remote	Select the required option to enable, disable, or make no change to system (remote).
	Debug	System	Select the required option to enable, disable, or make no change to Debug (system).

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

SSH Configuration Task

You can use the SSH system-defined task to configure SSH on devices.

The following device categories are supported by this task:

- IOS (including Cable devices)
- Content Engine
- CSS

- NAM

For more details, see Table 9-3.

You can enter the details of this task in the SSH Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For this task to work correctly, you must use any CLI-based protocol (Telnet or SSH) as the download protocol.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

Group	Sub-group	Field	Description
Common Parameters	Key Configuration	Action	Select the required option to enable, disable, or make no change to the key configuration.
IOS Parameters	Prerequisites		The Hostname and Domain name need to be configured for the devices.
	Key Configuration	Number of Key Bits [360-2048]	Enter the number of Key bits to be used for Key generation. The value must be between 360-2048 Key bits.
	Timeout	Action	Select the required option to add, remove, or make no change to the timeout value.
		Timeout Value [1-120):]	Enter timeout value for SSH sessions. The value should be between 1—120.
	Retries	Action	Select the required option to add, remove, or make no change to the number of retries.
		Number of Retries [1-5]	Enter the number of retries allowed. The number must be between 1—5.
CE Parameters	SSH Prerequisites	SSH Daemon	Select the required option to enable, disable, or make no change to the SSH daemon.
		Number of Key Bits [512-2048]	Enter the number of Key bits to be used for Key generation. The value must be between 512—2048 Key bits.
		SSH Timeout	Enter login grace time value in seconds for SSH sessions. Value must be between 1-99999.
		Password-guesses [1-99]	Specify the number of password retries allowed. The value must be between 1—99.
CSS Parameters		Number of Server Key Bits [512-32768]	Enter the number of Key bits to be used for Key generation. The value must be between 512—32768 Key bits.
	Port	Action	Select the required option to enable, disable, or make no change to the port configuration.
		Port Number [22-65535]	Enter the port number. This value can be between [22-65535]
		KeepAlive	Select the required option to add, remove, or make no change to keepalive.

For each device category, click on **Applicable Devices** to view the devices in your selection, to which this task applies.

TACACS Configuration Task

You can use the TACACS system-defined task to configure TACACS authentication.

This task supports the IOS device category including Cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the TACACS Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
Server Configuration		Action	Select to enable, disable, or make no change to the TACACS Server configuration.
		Hostname or IP Address	Enter the hostname or the IP address of the TACACS server.
Login Authentication		Action	Select to enable, disable, or make no change to the login authentication details.
	Credentials	Username	Enter the username. These values are entered in Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Password	Enter the enable password. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Re-enter the enable password. For details see Understanding the NetConfig Credentials Configuration Tasks.
IOS Parameters			
Server Retransmit		Action	Select to enable, disable, or make no change to the server retransmit configuration.
		Retries [0-100]	Enter the number of re-tries.
Server Timeout		Action	Select to enable, disable, or make no change to the server timeout value.
		Timeout [1-1000]	Enter the timeout value.
Enable mode Authentication		Action	Select to enable, disable, or make no change to the enable mode authenticating.
	Credentials	Username	Enter the username
		Password	Enter the enable password.
		Verify	Re-enter the enable password.

TACACS+ Configuration Task

You can use the TACACS+ system-defined template to configure TACACS+ on devices.

This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- Content Engine
- NAM

For more details, see Table 9-3.

You can enter the details of this task in the TACACS+ Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Group	Sub-group	Field	Description
Common Parameters			
TACACS Server Configuration	Server	Action	Select to enable, disable, or make no change to the TACACS Server configuration.
		Hostname or IP Address	Enter the hostname or the IP address of the TACACS server.
	Key	Action	Select to add, remove, or make no change to the TACACS encryption Key.
		Key	Enter the TACACS encryption key. The key is used to set authentication and encryption. This key must match the key used on the TACACS+ daemon. The key can be of any size.
		Verify Key	Re-enter the Key to confirm.
Login Authentication		Action	Select to enable, disable, or make no change to the TACACS+ authentication. • If login authentication is enabled, then when you try to login to the device, you are authenticated by the TACACS server. • If login authentication is disabled, then you are not authenticated by the TACACS server when you log in to the device.
	Credentials	Username	Enter TACACS+ username. These values are entered in the Device and Credential Repository only. They do not affect device configuration. For details see Understanding the NetConfig Credentials Configuration Tasks. Also see .
		Password	Enter TACACS+ password. For details see Understanding the NetConfig Credentials Configuration Tasks.
		Verify	Re-enter the password to confirm. For details see Understanding the NetConfig Credentials Configuration Tasks.

Group	Sub-group	Field	Description
IOS Parameters			
Enable mode Authentication		Action	Select to enable, disable, or make no change to the enable mode authenticating. Also see .
	Credentials	Password	Enter the enable password.
		Verify	Re-enter the enable password.
	List	Name	Enter default or named list.
		Set to Default	Select the set the default list.
	Type	(Drop-down list 1)	Select the required option: • No Choice • radius • tacacs+ • line • enable • local • none Similarly, select the type from the other three drop-down lists.
	New Model	Action	Select to enable, disable, or make no change to new model state.
CatOS Parameters			
Enable mode Authentication		Action	Select to add, remove, or make no change to the enable mode authentication.
	Credentials	Password	Enter the enable password.
		Verify	Re-enter the enable password.
	Server Options	Primary	Click to designate specified server as primary TACACS server.
		All	Click to clear all hosts from list of TACACS servers, if you selected remove in Action field.
ContentEngine Parameters	Server Option	Primary	Select to specify the server as primary.
	Password Option	ASCII Password	Select for an ACSII password.
	Connection Options	Timeout	Enter the timeout value.
		Retries	Enter the number of re-tries.
NAM Parameters			No category-specific commands **Note** The TACACS Server Key should be DES encrypted NAM devices.

At the time of enabling login authentication or enable mode authentication, it is mandatory for you to enter the username and password.

At the time of disabling login authentication or enable mode authentication, these fields are optional. While disabling login authentication or enable mode authentication, if username and password are not provided, then the corresponding fields in DCR are cleared and left blank.

This may make the device unreachable. Therefore we recommend that you provide the username and password at the time of disabling login authentication.

Telnet Password Configuration Task

You can use the Telnet Password system-defined configuration task to change the Telnet password on devices.

This task supports the following device categories:

- IOS (including Cable devices)
- Catalyst OS
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the Telnet Password Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

For details on the NetConfig credentials configuration tasks, see Understanding the NetConfig Credentials Configuration Tasks.

If you change the Telnet password on a Catalyst device with an RSM module using this template, the RSM Telnet password is also changed.

The fields in the Telnet Password Configuration dialog box are:

Group	Sub-group	Field	Description
IOS Parameters	Vty Lines	Action	Select an option to enable, disable, or make no change to the Vty Line password.
		Password	Enter the Vty Line password. If you select vty, change affects all device vty lines, and Device and Credential Repository is updated with new password.
		Verify	Re-enter the Vty Line password to confirm.
	Console Line	Action	Select an option to enable, disable, or make no change to the Console Line password.
		Password	Enter the Console Line password.
		Verify	Re-enter the Console Line password to confirm.
	Aux Line	Action	Select an option to enable, disable, or make no change to the Auxiliary Line password.
		Password	Enter the Aux Line password.
		Verify	Re-enter the Aux Line password to confirm.
CatOS Parameters	Telnet Password	Action	Select an option to enable, disable, or make no change to the telnet password. Device and Credential Repository is updated with new password.

Group	Sub-group	Field	Description
		Password	Enter the Telnet password.
		Verify	Re-enter the Telnet password to confirm.
		Apply command on modules Disable will set an empty password	Select this option to update only the non IP addressable modules. If you select the Action as Disable, the password will be removed.
PIX Parameters		Action	Select the required option to replace, reset, or make no change to the password.
		Password	Enter the password.
		Verify	Re-enter the password to confirm.
		Encrypted Password	Select this option, if the password you are entering is already encrypted.

Transform System-Defined Task

You can use the Transform system-defined task to configure IPSec on devices. You must configure the IKE configuration system-defined task before configuring the Transform system-defined task.

This task supports the following device categories:

- IOS (including Cable devices)
- PIX OS

For more details, see Table 9-3.

You can enter the details of this task in the Transform Set Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Transform Set Configuration dialog box are:

Group	Sub-Group	Field	Description
IOS Parameters			
Security Association Configuration	Seconds Configuration	Seconds [120-86400]	Enter number of seconds that will be used for negotiating IPSec SA.
		Remove	Select this option to remove any previously specified seconds value.
	Kilo Bytes Configuration	Kilo Bytes [2560-536870912]	Enter the amount of traffic in kilobytes that will be used for negotiating IPSec SA. Value must be between 2560-536870912.
		Remove	Select this option to remove any previously specified kilobytes value.

Group	Sub-Group	Field	Description
	IPSec Transform Set Configuration Note: Only for IOS 12.1 and higher.	Action	Select a required option to add, remove or make no change to transform set configuration. This sub-group of fields is applicable only to IOS version 12.1 and above.
		Transform Set Name	Enter a name for the transform set.
		Auth Header	Select the type of authentication algorithm.
		ESP Encryption	Select the type of encryption algorithm with ESP.
		ESP Authentication	Choose type of authentication algorithm with ESP.
		IP Compression	Select to use IP compression with LZS algorithm. This cannot be selected alone.
		Transport Mode	Select the mode of transport.
PIX Parameters			
Security Association Configuration		Seconds [120-86400]	Enter the number of seconds that will be used for negotiating IPSec SA. The value must be between 120—86400 seconds.
		Kilo Bytes	Enter the amount of traffic in kilobytes that will be used for negotiating IPSec SA. The value must be between 2560—536870912 kilo bytes.
IPSec Transform Set Configuration		Action	Select the required option to add, remove or make no change to transform set configuration.
		Transform Set Name	Enter name for the transform set.
		Auth Header	Select the type of authentication algorithm.
		ESP Encryption	Select the type of encryption algorithm with ESP.
		ESP Authentication	Select the type of authentication algorithm with ESP.
		IP Compression	Select to use IP compression with LZS algorithm. This cannot be selected alone.
		Transport	Select the mode of transport.

Web User Task

You can use the Web User configuration task to configure the web user for NAM devices. This is a system-defined task. For more details, see Table 9-3.You can enter the details of this task in the Web User Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).. The fields in the in the Web User Configuration dialog box are:

Group	Sub-group	Field	Description
NAM Parameters	Web User	Action	Select an option to add, remove, or make no change to the web user group of fields.
		Username	Enter the username of the web user.
		Password	Enter the password for the username.
		Verify	Re-enter the password to confirm.
	Privileges	Account Management	Select the required option to enable, disable or make no change to account management.
		System Config	Select the required option to enable, disable or make no change to system configuration.
		Capture	Select the required option to enable, disable or make no change to the capture configuration.
		Alarm Config	Select the required option to enable, disable or make no change to alarm configuration.
		Collection Config	Select the required option to enable, disable or make no change to the collection configuration.

Click **Applicable Devices** to view the devices to which this task applies.

Use-defined Protocol Task

You can use the User-defined Protocol task to configure the user-defined protocol on NAM devices. This is a system-defined task.

For more details, see Table 9-3.

You can enter the details of this task in the User-defined Protocol Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the in the User-defined Protocol Configuration dialog box are:

Group	Sub-group	Field	Description
NAM Parameters	User Defined Protocol	Action	Select an option to add, remove or replace the user-defined protocol.
		Protocol	Select the protocol: • TCP • UDP
		Port [0 - 65535]	Enter the port number. You can enter any port number in the range of 0—65535.
		Name	Enter the name of the user-defined protocol.

Group	Sub-group	Field	Description
	Affected Stats	Host	Select this option to enable host—Examines a stream of packets; produces a table of all network addresses observed in those packets (also known as the collection data). Each entry records the total number of packets and bytes sent and received by that host and the number of non-unicast packets sent by that host.
		Conversations	Select this option to enable host conversations.
		ART	Select this option to enable Application Response Time.

Click **Applicable Devices** to view the devices to which this task applies.

Cable BPI/BPI+ Task

You can use the Cable BPI/BPI+ Task to assign BPI/BPI+ options.

This task is applicable to the Cable device category. For more details, see Table 9-3.

You can enter the details of this task in the Cable BPI/BPI+ Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Cable BPI/BPI+ Configuration dialog box are:

Group	Sub-Group	Field	Description
BPI/BPI+	Interface Configuration	Cable Interface	Allows you to select an interface to modify the other fields. You must select at least one interface. Select the cable interface that you want to change.
		BPI	Select the appropriate option: • No Change—Does not change the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
	Key Lifetime	Action	Select the appropriate option: • No Change—Does not modify this option. • Replace—Modifies this option to your specification. • Default—Resets this option to the system default.

Group	Sub-Group	Field	Description
		KEK Lifetime [300 - 604800]	Replaces the time (in seconds) using your values or resets the time using the system default. Enter time in seconds to reset the time using your values. Enter a value from 300—604800 seconds and the default is 604800 seconds. Click to check the button to reset the field to system default.
		TEK Lifetime [180 - 604800]	Replaces the time (in seconds) using your values or resets the time using the system default. Enter time in seconds to reset the time using your values. The range is 180 - 604,800 seconds and default is 43,200 seconds. Click to check the button to reset the field to system default.
	BPI/BPI+ Options	Action	Select the required options: • No Change—Does not change the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
		Mandatory	Select to force all modems to use BPI.
		Authenticate Modem	Select to turn the BPI modem authentication on or off.
		Authorize Multicast	Select to turn BPI Multicast option on or off.
		OAEP Support	Select to enable or disable Optimal Asymmetric Encryption Padding (OAEP) BPI+ encryption.
		DSX Support	Select to enable or disable encryption for dynamic services SIDs.
		40 Bit Des	Select to indicate that you have chosen the 40 bit DES encryption. The system default is 56 DES encryption. This is Cisco's recommended encryption.

Click **Applicable Devices** to see the devices in your selection, that are applicable for this task.

For more information, refer to the following:

- http://www.cisco.com/warp/public/109/docsis_bpi.shtml
- hhttp://www.cisco.com/en/US/products/hw/cable/ps2211/prod_command_reference09186a00801a3ac4.html

Cable DHCP-GiAddr and Helper Task

You can use this task to configure the GiAddr field of DHCPDISCOVER and DHCPREQUEST packets with a relay IP address before they are forwarded to the DHCP server. You can apply this task only for a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 9-3.

You can enter the details of this task in the Cable DHCP-GiAddr and Helper Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note At a time, you can apply this task only to a single device, because cable templates configure interfaces on devices.

The fields in the Cable DHCP-GiAddr and Helper Configuration dialog box are:

Group	Sub-Group	Field	Description
Config Setup		Cable Interface	Select a cable interface to make the configuration changes to the selected interface, from the drop-down list. If there are no interfaces available, you will see the option No Interfaces Found in the drop-down list. You should make sure that the device is reachable and then select a valid interface.
		Action	Select an option from the drop-down list. The options are: • No Change—Does not change the current configuration. • Add/Modify—Adds a new GiAddr or Helper Address or both, or modifies an existing GiAddr or Helper Address or both.· • Remove—Removes the GiAddr or Helper Address or both.
			Select an option to Add or Modify, from the drop-down list: • DHCP-Giaddr & Helper-Address—Enables you to set the DHCP GiAddr to Policy or Primary. You can also specify values for the fields in the Cable Helper Addresses group. • DHCP-Giaddr—Enables you to set the DHCP GiAddr to Policy or Primary. • Helper-Address—Enables you to specify values for the fields in the Cable Helper Addresses group.
	Cable DHCP Giaddr	Policy Primary	Allows you to set the DHCP GiAddr to Policy or Primary: • Policy—Selects the control policy, so the primary address is used for cable modems and secondary addresses are used for hosts. • Primary—Always selects the primary address for GiAddr field. Enable this field by selecting Helper Address.

Group	Sub-Group	Field	Description
	Cable Helper Addresses	Helper Address	Allows you to enter the Helper Address to Cable Modem, Host or Host & Cable Modem.
		• Cable-Modem • Host • Host & Cable-Modem	• Cable-Modem—Specifies that only Cable Modem UDP broadcasts are forwarded. • Host—Specifies that only host UDP broadcasts are forwarded. • Host & Cable Modem—Specifies that both host and cable modem broadcasts are forwarded. Enable this field by selecting Action as DHCP GiAddr & Helper Address or by selecting Action as Helper Address.

Click **Applicable Devices** to view the devices to which this task applies.

Cable Downstream Task

You can use this task to configure the Annex, Channel-ID, Frequency, Modulation, Interleave depth, and Set rate limit of downstream cable interface. You can also configure the Radio Frequency (RF) output of a downstream cable interface on a Cisco uBR7100 router.

This task is applicable only to Cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the Downstream Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note You can apply this task to only a single Cable-CMTS device at a time.

The fields in the Downstream Configuration dialog box are:

Group	Sub-Group	Field	Description
Cable Parameters		Cable Interface	Select the required option from the drop-down list. Select a cable interface to make the required configuration changes. If you do not want to select any cable interface, choose the Not Selected option.
Activate/ Configure	Shutdown	Action	Allows you to shutdown or activate the selected interface. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • Shutdown—Deactivates the DS port. • No Shutdown—Activates the DS port.

Group	Sub-Group	Field	Description
	Interleave Depth	Interleave Depth	Allows you to select the interleave depth of a channel between 8 - 128. The default is 32. Specify the interleave depth by selecting the appropriate option from the drop-down list.
		Remove	Select to remove the interleave depth configuration.
	Framing Format	MPEG Framing Format	Select the MPEG framing format from the drop-down list. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • Annex A—For Cisco uBR-MC16E cable interface card and Cisco uBR7111E and Cisco uBR7114E Universal Broadband Routers. • Annex B—For all other Cisco cable interface cards.
		Remove	Select to remove a previously-specified MPEG framing format configuration.
	Modulation	Modulation	Sets the modulation for a downstream port on a cable interface. Select the required option. The options are: • No Change—Does not allow modification of any fields in this sub-group of fields. • 64 qam • 256 qam
		Remove	Select to remove a previously-specified modulation configuration.
	Channel	Channel ID (0-255):	Channel-ID can be from 0-255. Specify the channel-ID.
		Remove	Select to remove the Channel ID.
	Frequency	Frequency (54-858 MHz)	Frequency range can be from 54MHz -1,000MHz. Enter the frequency.
		Remove	Select to remove a previously-specified frequency range.
Traffic Shaping		Rate Limit	Select the required option from the drop-down list. The options are: • No Change—Does not allow modification of any fields in this group of fields. • Enable—Enables this option. • Disable—Disables this option.

Group	Sub-Group	Field	Description
		Rate Limit Algorithm (Optional):	• None—Does not modify the rest of the fields. • Token-bucket with DS Traffic Shaping—Modifies the Token Bucket Algorithm option. • Token-bucket without DS Traffic Shaping—Modifies the Token Bucket without DS Traffic Shaping Algorithm option • Weighted-discard—Modifies the Weighted Discard option.
	Token Bucket (Optional)	Granularity in Milli seconds (Optional):	Specifies traffic shaping granularity in milliseconds. This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffice Shaping. Select the required value from the drop-down list. You can choose a value between 1—16 msec.
		Max Delay in Milli seconds (Optional):	Sets the maximum buffering delay in milliseconds. This field is enabled only if you have selected the Rate Limit Algorithm as Token-bucket with DS Traffice Shaping. Select the required value from the drop-down list. You can choose a value between 128 to 1024.
	Weighted Discard (1-4) (Optional)	Weight for the exponential moving average of loss rate	Sets the weighted discard algorithm. This field is enabled only if you have selected the Rate Limit Algorithm as Weighted Discard. Enter a weight between 1 - 4.

Click **Available Devices** to view the list of devices from your selection, to which this task applies.

Cable Upstream Task

Use this task to configure the frequency, minislot size, power level and admission control on upstream cable interfaces. You can apply this task only for a single Cable-CMTS device at a time.

This task is applicable only to Cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the Upstream Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note You can apply this task to only a single cable device at a time.

The fields in the Upstream Configuration dialog box are:

Group	Sub-Group	Field	Description
Config Setup		Cable Interface	Allows you to select cable interfaces for configuration. Select the cable interfaces from the drop-down list.
	Activate/ Deactivate US Port	Activate/Deactivate	Select one of these options from the drop-down list. The options are: • No Change—Does not change the existing configuration. • Shutdown—Deactivates this port. • No Shutdown—Activates this port.
Frequency		Value [5-42 MHz]	Enter the required frequency value in the range 5—42 MHz. The range for the frequency is: • 5—65 MHz for Cisco uBR-MC16E cable interface line card • 5—42 MHz for all other cable interface line cards.
		Set to Default	Select this option to set the default frequency. A negation command is generated to remove the frequency value and set the default. This is because the default frequency value is dynamic and varies from device to device.
Power Configuration	Power Level	Value [-10-+25 dBmV]:	Enter the power level. The valid range for the power level is between -10dBmV—+25dBmV.
		Set to Default	Select this option to set the default power level. The default is 0dBmV.
	Power Adjustment	Continue [2-15 dB]	Enter the power adjustment value. The valid range for power adjust value between 2dB—15dB.
		Set to Default	Select this option to set the default power adjustment value. The default is 2dB.
		Noise	Enter the power adjust noise level. The valid range for the power adjustment noise value between 10 - 100%.
		Set to Default	Select this option to set the default noise value. The default is 30%.
		Threshold [0-10 dB]	Enter the power adjustment threshold value. The valid range for the power adjustment threshold value between 1dB - 10dB.
		Set to Default	Select this option to set the default power adjustment threshold value. The default is 1dB.
Admission Control		Value [0 - 1000%]	Indicates the maximum cumulative bandwidth reservation allowed before new CMs are rejected. The valid range is between 10%—1000%.
		Set to Default	Select this option to set the default admission control value. The default value is 100%.

Group	Sub-Group	Field	Description
Minislot Size		Size	Select the required options. The options are: • No Change • 2 • 4 • 8 • 16 • 32 • 64 • 128 • [default] Select **No Change** to make no changes in this field.
Channel Width(Hz)		Size	Select the required channel width option. The options are: • No Change—Does not modify the existing configuration. • 200000 • 400000 • 800000 • 1600000 (default) • 3200000 Select **No Change** to make no changes in this field.
Concatenation		Concatenation	Select one of these options: • No Change—Does not modify the existing configuration • Enable—Enables this option. • Disable—Disables this option.
FEC		FEC	Select one of the following options for Enable Forward Error Correction (FEC): • No Change - Does not modify the existing configuration. • Enable - Enables this option. • Disable - Disables this option.
Fragmentation		Fragmentation	Select the required fragmentation option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option.
Rate Limit		Rate Limit	Select the required rate limit option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option.

Group	Sub-Group	Field	Description
		Apply Token Bucket Algorithm	Click the check box to apply this option.
		Enable Traffic Shaping	Click the check box to apply this option.
Data Backoff		Data Backoff	Select the required data backoff option. The options are: • No Change—Does not modify the existing configuration. • Enable—Enables this option. • Disable—Disables this option. If you choose Enable, you can perform data back off automatically, or manually by entering the start and end values.
		Automatic	Choose this to apply a default value for data automatically.
		Start Value [0-15]	Enter the start value. The valid range for the start value is 0—15. there is no default value.
		End Value [0-15]	Enter the end value. The valid range for the end value is 0—15. there is no default value.
Range Backoff		Range Backoff	Select one of these options: • No Change—Does not modify the existing configuration. • Enable—Allows you to perform data back off automatically, or manually by entering the start and end values. • Disable—Disables this option.
		Automatic	Select this, to apply a range back-off value automatically.
		Start Value (0-15)	Enter the start value. The valid range for the start value is 0-15. There is no default value.
		End Value (0-15)	Enter the end value. The valid range for the start value is 0-15. There is no default value.

Click **Available Devices** to view the list of devices from your selection, to which this task applies

Cable Interface Bundling Task

You can use this task to configure the interface bundling. You can apply this task only to a single Cable-CMTS device at a time.

This task is applicable to the Cable device category. For more details, see Table 9-3.

You can enter the details of this task in husbanded Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

Note At a time, you can apply this task only to a single device, because cable templates configure interfaces on devices.

The fields in the Bundle Configuration dialog box are:

Group	Field	Description
Cable Parameters	Action	Select one of these options: • No Change—Does not modify the existing parameters. • Add—Enables you to configure a interface as a master interface or a slave interface. • Remove—Enables you to change the previous configuration of the interface (master to slave or vice versa). Choose the option from the drop down list.
	Bundle ID (1-255)	Indicates the bundle identifier. Enter a bundle ID between 1 - 255.
	Master Interface	Allows you to configure the primary interfaces. Select the cable interface from the list of primary interfaces. Select **Not Selected** if you do not want to select a primary interface.
	Slave Interface	Allows you to configure the secondary interfaces. Select the cable interface from the list of secondary interfaces. Select **Not Selected** if you do not want to select a secondary interface.

Click **Applicable Devices** to view the devices to which this task applies.

Cable Spectrum Management Task

You can use this task to create and assign spectrum groups to cable interfaces and upstream interfaces.

This task supports cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the Cable Spectrum Management Configuration dialog box. To invoke this dialog box, see Starting a New NetConfig Job.

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Cable Spectrum Management Configuration dialog box are:

Group	Sub-Group	Field	Description
Spectrum Management	Spectrum Group	Action	Select one of these options: • **No Change**—Does not allow you to make any changes in the Spectrum group of fields. • **Add**—Allows you to add options. • **Remove**—Allows you to remove options.
		Spectrum Group ID [1 - 32]	Enter the Spectrum Group ID. The range for Spectrum Group ID is between 1—32.
		Frequency Setting	Select one of these frequency settings: • Band—Enter a range of frequencies. • Fix—Enter a fixed frequency.
		Start Frequency [5 - 42 MHz]	Enter the start frequency. The range of frequencies is: • 5MHz—65MHz for Cisco • uBR-MC16E cable interface card • 5MHz—42MHz for all other cable interface cards
		End Frequency [5 - 42 MHz]	Enter the end frequency. • The range of frequencies is: 5MHz—65MHz for Cisco • uBR-MC16E cable interface card • 5MHz—42MHz for all other cable interface cards. This field is enabled only if you choose **Fix** as the value in the Frequency Setting filed, in the Spectrum Group.
	Optional Configuration	Power Level [-10 - 25 dBmV]	Enter the Power Level. The valid power levels are between -10dBmV - +25dBmV. The default is 0dBmV.
		Hop Period [5 - 300 Sec]	Enter the Hop period. The valid range for a Hop Period (in seconds) is between 1-3600. The default for Advanced Spectrum Management is 25 seconds. For all others, the default is 300 seconds. This field is enabled only if you choose **Add** as the value in the Action field, in the Spectrum Group.
		Hop Threshold [0 - 100%]	Enter the Hop Threshold. The valid range for Hop Threshold is between 1 - 100%. The default is 20%. This field is enabled only if you select **Add** as the value in the Action field, in the Spectrum Group.
		Shared RF Spectrum Group Configuration	Indicates the upstream ports in a spectrum group can share the same upstream frequency.

Group	Sub-Group	Field	Description
	Schedule	Schedule	Select one of these options from the drop down list: • **No Change**—Does not allow you to enter the scheduling information. • **Add**—Allows you to add a scheduled task. • **Delete**—Allows you to delete a scheduled task.
		Schedule Day	Select the schedule day from the drop-down list.
		Schedule Time (hh:mm:ss)	Enter the schedule time in the hh:mm:ss format.
	Interface Assignment	Action	Select one of these option from the drop-down list: • **No Change**—Does not allow changes to the existing assignment. • **Assign**—Allows you to assign an interface. • **Unassign**—Allows you to unassign an interface.
		Cable Interface	Select a cable interface from the drop-down list.
		Spectrum ID [1 - 32]:	Enter the Spectrum ID. The range for Spectrum ID is between 1—32. This field is disabled if you chose **Unassign** as the value in the Action field, in the Interface Assignment sub-group.

Click **Applicable Devices** to view the devices to which this task applies.

Cable Trap Source Task

You can use this task to configure SNMP Traps hosts, notification, message and notification of SNMP Traps on a cable interface.

This task supports cable devices.

For more details, see Table 9-3.

You can enter the details of this task in the Trap Source Configuration dialog box. (To invoke this dialog box, see Starting a New NetConfig Job.)

For the features of system-defined tasks and a description of the features of a system-defined task dialog box, see Understanding the System-defined Task User Interface (Dialog Box).

The fields in the Trap Source Configuration dialog box are:

Group	Sub-Group	Field	Description
Trap Source Configuration	Trap Source Interface	Action	Select the required option to add, remove or make no change to a Trap Source interface.
		Trap Source Interface	Select the required trap source interface from the drop-down list.
	CM On/Off Trap Interval	Cable Interface	Select the cable interface on which to specify the trap interval.

Group	Sub-Group	Field	Description
		Interval [0 - 86400]	Specify a value for the trap interval in the range 0—86400 seconds.
		Set to Default	Select this to set the trap interval to the default value of 600 seconds.

Click **Applicable Devices** to view the devices to which this task applies.

cwcli netconfig

This command is described in the cwcli framework chapter. For details see the topic Running the cwcli netconfig Command in the section CLI Utilities.

CHAPTER 10

Editing and Deploying Configurations Using Config Editor

The Config Editor option of the Configuration tab of Resource Manager Essentials, provides easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file that exists in the configuration archive.

The Configuration Management application stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the Inventory. It automatically tracks changes to configuration files and updates the database if a change is made.

You can open the configuration file, change it, and download it to the device.

- To start Config Editor from the CiscoWorks desktop, select **RME > Config Mgmt > Config Editor**.

  The Config Editor window appears.
- To set user preferences in Config Editor from the CiscoWorks navigation tree, select **RME > Admin > Config Mgmt > Config Editor**.

  The User Preferences window appears.

Config Editor Tasks

Config Editor users can:

- Open a configuration file version of a device for editing.
- Open configuration file version based on search criteria.
- Open an external configuration file.
- Save modified configuration file in private work area on the server and open the saved file when required.
- Save a configuration file in a public location.
- Send configuration file to syntax checker utility.
- Deploy configuration files to the device.
- Send configuration download jobs for approval.
- View all download jobs and perform job management operations.
- List out all the modified files, allow the user to select and download or close the configuration.

- Compare configurations that they are editing with the original configuration file version and other configuration versions of the selected device.
- Open a baseline configuration stored in config archive.

For the new features in this release, see What's New in this Release.

Benefits of Configuration Editor

Config Editor allows you to edit and download configuration files to devices using a GUI instead of the command line interface (CLI). Use Config Editor to edit individual device configurations within RME and then download them back to a device.

A copy of the updated configuration will automatically be stored in the Configuration Archive.

Figure 10-1 Config Editor Functional Flow

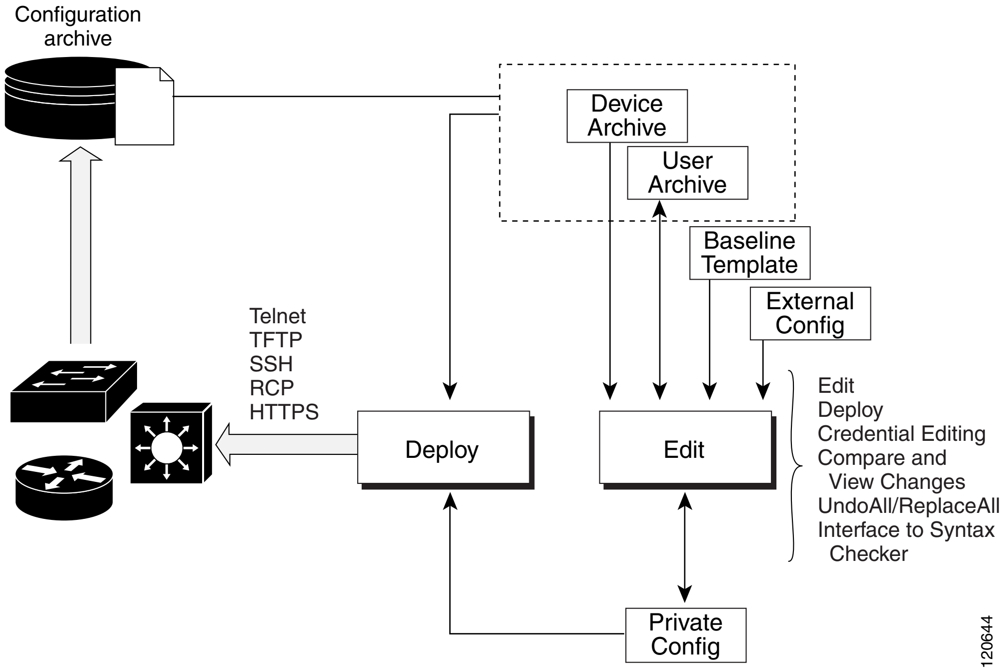

Configuration archive
Device Archive
User Archive
Baseline Template
External Config
Telnet
TFTP
SSH
RCP
HTTPS
Deploy
Edit
Edit
Deploy
Credential Editing
Compare and View Changes
UndoAll/ReplaceAll
Interface to Syntax Checker
Private Config
120644

Table 10-1 shows the tasks you can accomplish with the Config Editor option.

Table 10-1 Config Editor Tasks

Task	Description	Action
Open a configuration file.	Open a configuration file for editing. You can open a configuration file in four ways: • Device and Version • Pattern Search • Baseline • External Location	Select RME > Config Mgmt > Config Editor > Config Files.
Edit configuration files from the archives.	Edit a configuration file from the archive.	Select RME > Config Mgmt > Config Editor > Config File> Device and Version > Edit.
Edit a configuration file by pattern	Edit a configuration file by searching for a pattern. A pattern can be any text string.	Select RME > Config Mgmt > Config Editor > Config File > Pattern Search > Finish.
Edit a configuration file by baseline template	Create a baseline configuration from the baseline template maintained in configuration archive.	Select RME > Config Mgmt > Config Editor > Config File > Baseline > Finish.
Edit a configuration file by external location	Associate a device with the selected configuration file from an external location in the server.	Select RME > Config Mgmt > Config Editor > Config File > External Location> Edit.
Print configuration files.	Print a configuration file.	1. Select RME > Config Mgmt > Config Editor. 2. Select the configuration file and click **Edit**. 3. Select the Print icon at the top right corner.
Remove configuration file from the private area	Remove a configuration file in the private work area on the server.	1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit**. 3. Click **Delete**.
Remove a configuration from the public work area	Remove a configuration file in the public work area on the server.	1. Select RME > Config Mgmt > Config Editor > User Archive**.** 2. Select the configuration file and click **Edit**. 3. Click **Delete**.
Save a configuration file in the public work area.	Save an edited configuration file in the public work area on the server and retrieve the saved file when required.	1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit.** 3. Click **Save**.

Table 10-1 Config Editor Tasks (continued)

Task	Description	Action
Save a configuration file in the private work area.	Save an edited configuration file in the private work area on the server and retrieve the saved file when required.	1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Save**.
Undo editing or typing changes	Undo editing or typing changes when editing a file. You can undo editing changes of a file in private or public work areas.	To undo editing changes of a file in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Undo All**. To undo editing changes of a file in the public work area: 1. Select **RME > Config Mgmt > Config Editor > User Archive.** 2. Select the configuration file and click **Edit.** 3. Click **Undo All**.
Find and replace text	Find and replace all occurrences of the text when editing a configuration file in the raw mode or find the text in a particular configlet in the processed mode	To find and replace text of a file in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs 2. Select the configuration file and click **Edit**. 3. Click **Replace All**. To find and replace text of a file in the public work area: 1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit**. 3. Click **Replace All**.
Export Configuration File Changes	Exporting Changes of a Configuration File to a PDF file.	1. Select RME > Config Mgmt > Config Editor. 2. Select the configuration file and click **Edit.** 3. Select the **Export icon** at the top right corner.
Close Configuration File	Close a configuration file.	To close a configuration file in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Close**. To close a configuration file in the public work area: 1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit.** 3. Click **Close**.

Table 10-1 Config Editor Tasks (continued)

Task	Description	Action
Configure Job Policies.	Configure a default policy for job properties that applies to all future jobs. You can also specify whether the property can be modified when the job is created.	Select Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies > Config Editor.
Set up the default editing mode.	Set up or change your default editing preferences. Config Editor remembers your preferred mode even across different invocations of the application. You can also change the mode when you open a configuration file using the Device and Version option. However, Config Editor does not remember this change across different invocations of the application. Only the changes made using the Admin tab is remembered.	Select RME > Admin > Config Mgmt > Config Editor.
View changes.	View the changes made to the opened configuration file. RME compares the edited file with the original version.	To view changes made to a configuration file in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **View Changes**. To view changes made to a configuration file in the public work area: 1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **View Changes**.

Table 10-1 Config Editor Tasks (continued)

Task	Description	Action
Compare versions of the configuration files.	Compare the edited file with any version in the Configuration Archive.	To compare versions of configuration files in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **Compare Config**. To compare versions of configuration files in the public work area: 1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit.** 3. Click **Tools**. 4. Select **Compare Config**.
View list of modified files.	View a list of files edited files by all users in private or public work areas.	• To view a list of modified configuration files in private work area, select RME > Config Mgmt > Config Editor > Private Configs. • To view a list of modified configuration files in public work area, select RME > Config Mgmt > Config Editor > User Archive.
Browse and edit Config Editor jobs.	Browse the Config Editor jobs that are registered on the system and edit them as necessary.	Select RME > Config Mgmt > Config Editor> Config Editor Jobs > Edit.
View job details.	View detailed information about a registered Config Editor job and perform job management operations. You can also edit a job from its detailed view.	Select RME > Config Mgmt > Config Editor> Config Editor Jobs.
Deploy a config	Define a deploy job. Defines jobs to deploy configuration files to the device.	Select RME > Config Mgmt > Config Editor> Config Editor Jobs > Create.
Copy a job	Copy a job	Select RME > Config Mgmt > Config Editor > Config Editor Jobs > Copy.
Delete a job	Delete a job	Select RME > Config Mgmt > Config Editor> Config Editor Jobs > Delete.
Stop a job	Stop a job	Select RME > Config Mgmt > Config Editor > Config Editor Jobs > Stop.

Table 10-1 Config Editor Tasks (continued)

Task	Description	Action
Check the configuration file syntax.	Check the syntax of the configuration file with external syntax checker that is registered in CMIC Link registration.	To check the configuration syntax of a file in the private work area: 1. Select RME > Config Mgmt > Config Editor > Private Configs. 2. Select the configuration file and click **Edit.** 3. Click **Tools** 4. Click **External Syntax Checker**. To check the configuration syntax of a inthe public work area: 1. Select RME > Config Mgmt > Config Editor > User Archive. 2. Select the configuration file and click **Edit.** 3. Click **Tools** 4. Click **External Syntax Checker**.
Update DCR after deploy	Updating DCR after successfully deploying credential commands. This is applicable only for Telnet/SSH based download.	User configurable. An option is provided in the job creation flow.

Setting Up Preferences

You can use this feature to set up your editing preferences. Config Editor remembers your preferred mode, even across different invocations of the application.

You can change the mode using the Device and Version, Pattern Search, Baseline or External Configuration option but the changes do not affect the default settings.

To set up preferences:

Step 1 Select **RME > Admin > Config Mgmt > Config Editor**.

The User Preferences dialog box appears.

Step 2 Set the default edit mode:

- Select **Processed** to display the file in processed mode.

  The configuration file appears at the configlet level (a set of related configuration commands). The default is Processed.

- Select **Raw** to display the file in raw mode.

  The entire file appears as shown in the device.

Step 3 Click **Apply** to apply the set preferences.

Overview: Editing a Configuration File

The Editor is a core component in Config Editor. It acts as the interface to open a configuration file, make a local copy, save the changed configuration and commit the changes back to original location.

You can edit a file by:

- Selecting device and version of configuration file
- Searching for a pattern
- Selecting a baseline configuration file
- Selecting a configuration file stored in an external location

You can edit a previously opened file, that is, a file from your private area or public work area.

You can edit the files in either the Raw or Processed mode.

- Raw mode—The entire file is displayed. After you open a file in a specific mode, you can view it only in that mode.
- Processed mode—Only the file commands are displayed at the configlet (set of related configuration commands) level.

Working With the Configuration Editor

You can use the editor to:

- Edit and save changes to the configuration file in public or private work area.
- Undo editing or typing changes
- Replace a string in opened configuration files
- Compare configuration files with the same device configuration
- View changes made in the configuration file
- Run Syntax Checker

The Editor window opens in Raw or Processed mode, based on your preferences.

To launch the Editor:

Step 1 Select **RME > Config Mgmt > Config Editor**.

Step 2 Open a configuration file using any of the following methods:

- Using the selection criteria. See Overview: Opening a Configuration File
- Using Private Configs
- Using User Archive
- Using Device Center

Using Private Configs

a. Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

b. Select the configuration and click **Edit.**

Using User Archive

a. Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

b. Select the configuration and click **Edit.**

Using Device Center

a. In the CiscoWorks LMS Portal home page, select **Device Troubleshooting > Device Center**.

The Device Center dialog box appears.

b. Select a device using device selector.

The functions available appears.

c. Select **Management tasks > Edit config**

The Editor window appears.

Step 3 Edit the credential commands in the raw or processed mode. See Processed Mode and Raw Mode.

Step 4 Select any of the following:

- **Save** to save changes to the configuration file. See Saving a Configuration File.
- **Save As** to save changes to the configuration file to a specified location.
- **Undo All** to undo editing or typing changes. See Undoing All.
- **Replace All** to replace a string in the opened configuration files. See Replacing All.
- **Tools...** to launch the Config Editor tools. See Selecting Configuration Tools.
- **Close** to close the Config Editor window. See Closing a Configuration File.

Processed Mode

The configuration file appears at the configlet level (a set of related configuration commands). The default is Processed.

In the Processed mode, Editor window is divided into two panes.

- The left pane displays the configuration tree according to the grouping of configlets.
- The right pane displays the commands of configlets in two sections:
  - The lower section, called the credential area contains all the credential commands with the credentials masked. Click on the encrypted link to modify credentials.
  - The upper section, called the non-credential area contains only non-credential commands. The non-credential commands are editable.

Raw Mode

The entire file appears as shown in the device. After you open a file in a specific mode, you can view it only in that mode.

In Raw mode there are two sections for the entire configuration.

- The upper section, called the non-credential area contains only non-credential commands. The non-credential commands are editable.
- The lower section contains all the credential commands with the credentials masked. The credential commands can be edited.

Note Do not delete or edit the placeholder that describes the credential position. If you do so, the file generates errors.

Editing Configuration Files by Handling Interactive Commands in Config Editor Jobs

An interactive command is the input you will have to enter, after a command runs.

For example, in the case of Catalyst 5000 series devices, the command is:

```
set vtp v2 enable
```

This command enables version 2 of VTP on the device. This command is an interactive command and requires user intervention after running the command.

You can download this command through ConfigEditor using:

```
#INTERACTIVE

set vtp v2 enable<R>y

#ENDS_INTERACTIVE
```

In Resource Manager Essentials, such commands can be included in config jobs run using Config Editor. You can handle interactive commands by editing configuration files.

To edit configuration files using interactive commands:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Click **Edit.**

The Editor window appears.

Step 3 Enter an interactive command in the configuration file, in the upper section that contains only non-credential commands using the following syntax:

```
#INTERACTIVE

command1<R>response1<R>response2
```

```
command2<R>response1<R>response2<R>response3

command3<R>response1

command4<R>response1<R>response2

#ENDS_INTERACTIVE
```

`<R>` tag is case-sensitive and this must be entered in uppercase only.

Step 4 Enter modification comments in the Change Description field.

Modifying Credentials

You can use this feature to modify or delete the credentials of a configuration file.To do this:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Click **Edit.**

The Editor window appears.

Step 3 Click the masked credential link in the With Credentials pane. (The masked credential appears as multiple *s.)

The Modify Credentials dialog box appears.

Step 4 Enter the information required to modify credentials.

Field	Description
Modify	Modifies credentials of the selected configlets.
Delete	Deletes the existing credentials of the selected configlets.
Modify Mode	
Old Credential	Old credential appears in clear text in a non-editable text box.
New Credential	Enter the new password of the selected configlets. This field is editable when you select the Modify option.
Confirm Credential	Enter the new password of the selected configlets again to confirm the new value. This field is editable when you select the Modify option.

Step 5 Click **Submit** to record changes.

The changes are reflected in the Editor window.

Step 6 Enter modification comments in the Change Description field.

Removing a Configuration File

You can use this feature to remove configuration files from private work area or public work area using Config Editor.

To remove a configuration file stored in the private work area:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs**.

The List of Private Configs window appears.

Step 2 Select the configuration file(s) that needs to be removed.

Step 3 Click **Delete**.

To remove a configuration file stored in the public work area or the user archive:

Step 1 Select **RME > Config Mgmt > Config Editor > User Archive**.

The User Archived Configs window appears.

Step 2 Select the configuration file(s) that needs to be removed.

Step 3 Click **Delete**.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Saving a Configuration File

You can use this feature to save your changes to the configuration file. The changes can be saved in either private area or public area. You can open the file later to modify it or to deploy it to the device.

To save a configuration file:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Save**.

The Save Config dialog box appears, only if you are saving the configuration file for the first time. The subsequent saving of a file is done directly to its previously saved location.

Step 4 Enter the information required to save a configuration file.

Field	Description	Usage Notes
Public	Saves the files in the public area.	None.
Private	Saves the files in the private area.	When a configuration from list of private config is opened and saved in the public area (user archive) with the same name as the private configuration, the private configuration with that name gets deleted. However, the reverse is not true. That is when a config is opened from the public area (user archive) location and saved in the private area, the public configuration is not deleted.
Branch Name	Name of branch.	Private area for you where configuration files are stored locally.

Step 5 Click either:

- **Submit** to save the configuration file.

  Or
- **Cancel** to return to the previous setting.

After the configuration file opened from Device Archive is saved to the private or public (user archive), all the subsequent operations (compare, show changes) behave as if the configuration is opened from a private or public location.

Undoing All

You can use this feature to undo editing or typing changes. To do this:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Edit the configuration file.

Step 4 Click **Undo All**.

A message window appears with the message:

```
Do you want to discard all the changes?
```

Step 5 Click either:

- **OK** to return to the last saved configuration file.

  Or

- **Cancel** to avoid making any changes.

Replacing All

You can use this feature to search for and replace text in the file. To do this:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Replace All**.

The Replace All dialog box appears.

Step 4 Enter the text to search for in the Find field.

Step 5 Enter the replacement text in the Replace With field.

Step 6 Click either:

- **Replace All** to replace all instances of the text in the text area.

  Or

- **Cancel** to avoid making any changes.

Printing a Configuration File

You can use this feature to print the configuration file. To do this:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Select the **Print** icon at the top right corner.

A new browser window appears. The details are in PDF format. You can print the information, using the Print option provided by the browser.

Exporting Changes of a Configuration File

You can use this feature to export the configuration file to PDF format. To do this:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Select the **Export** icon at the top right corner.

A new browser window appears. The details are in PDF format.

Deploying a Configuration File

You can use this feature to deploy a configuration file to a device.

To deploy a configuration file:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location. For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Deploy.**

The Job Option Details dialog box appears.

Step 3 Enter the following information:

Field	Description
Job Information	
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Job Options	

Field	Description
Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and device Enable password or – Disable the Job Password option in the Job Schedule and Options dialog box.
Deploy Mode	
Overwrite	Select the **Overwrite** option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (RME assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same. Overwrite mode supports Write2Run of the configuration only.
Merge	Select the **Merge** option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device. Merge mode supports both Write2Run and Write2Start of the configuration.

Step 4 Click **Submit**.

An immediate Deploy of Configuration on Device job will be scheduled.

A message appears, `Job` *ID* `is created successfully`.

Where *ID* is a unique Job number.

Step 5 Click **OK**.

You can check the status of your scheduled *Config Editor Deploy* job by selecting **RME** > **Config Mgmt** > **Config Editor > Config Editor Jobs**.

- Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device.

- Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.

Closing a Configuration File

You can use this feature to close the configuration file without exiting the application. If the file contains unsaved changes, you are prompted to save before closing.

To close the configuration file:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Close**.

If the file contains any unsaved changes, a message window appears with the message:

```
You have done some changes since last save. Do you want to the save the changes?
```

Step 4 Click either:

- **OK** to save the configuration file in a private area.

  Your changes are saved.

  Or

- **Cancel** to ignore your changes.

Selecting Configuration Tools

You can use this feature to choose a configuration tool from the list of configuration tools. The list of configuration tools available are as follows:

- Comparing Versions of Configuration Files
- Displaying Your Changes
- Overview: Syntax Checker

To select a configuration tool:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools.**

The Select Tool dialog box appears with the following tools:

Option	Description
Compare Config	Compares the current file with any earlier version in the configuration archive.
View Changes	Displays the changes made in the opened file.
External Syntax Checker	**1.** Select this option to check the configuration file using an external syntax checker that is registered with Cisco Management Integration Center (CMIC). **2.** Click **Submit**. Config Editor launches the URL, displaying the configuration commands and sysobject ID of the device as input to the external syntax checker. **3.** View the output displayed by the external syntax checker. **4.** Modify the commands in Config Editor.

Step 4 Select a tool.

Step 5 Click either:

- **Submit** to launch the tool.

Or

- **Cancel** to close the window.

Comparing Versions of Configuration Files

You can use this feature to compare the current file with any earlier version in the configuration archive.

The Compare option is enabled only if a file is open.

To compare versions of configuration files:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools.**

The Select Tool dialog box appears.

Step 4 Select **Compare Config**.

Step 5 Click either:

- **Submit** to view the Version Selector dialog box and proceed to the next step.

  Or

- **Cancel** to close the window without making any changes.

Step 6 Select a version with which you want to compare the current open file, from the list of other versions.

The Configuration Compare Report appears.

Step 7 Select the View mode.

Step 8 Click **Processed** to display files in processed mode. This is the default option.

Files appear at the configlet level (a set of related configuration commands).

Step 9 Click **Raw** to display the files in raw mode.

The entire file appears.

If you want to print the report, click **Print**.

Displaying Your Changes

You can use this feature to display the changes made in the opened file. The text file in archive is compared with the opened version.

The View Changes option is enabled only if a file is open

To display the changes in the open file:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Select the configuration file and click **Edit.**

The Editor window appears.

Step 3 Click **Tools**.

The Select Tool dialog box appears.

Step 4 Select **View Changes** option.

Step 5 Click either:

- **Submit** to view the differences in a new window.

Or

- **Cancel** to close the window without making any changes.

Overview: Syntax Checker

Config Editor provides ways to check the syntax of config commands using syntax checker. Config Editor checks syntax using the Interface to External Syntax Checker.

Interface to External Syntax Checker

The external syntax checker has to be registered with Cisco Management Integration Center (CMIC) using Link Registration.

For details see, Registering an External Syntax Checker Application With CMIC. Config Editor queries CMIC to check if the application is registered with the name “Config Syntax Checker”.

If the application is registered, Config Editor knows the External Syntax Checker URL to be launched and parameters to be passed to the syntax checker.

Config Editor launches the URL with two parameters, deviceSysObjID and cfgCmds:

- **deviceSysObjID**—sysObjectID of the device. External Syntax Checker uses deviceSysObjID to identify the device type.
- **cfgCmds**—List of commands for which the syntax has been checked.

ConfigEditor launches the External Syntax Checker URL in POST method. When the URL is launched you can view the configuration commands for which the syntax has been checked.

To validate the results and correct the commands in Config Editor:

Step 1 Go to the CiscoWorks LMS Portal homepage and select **RME > Config Mgmt > Config Editor > Config Files**.

Step 2 Select **Device and Version** in the Selection Area page.

Step 3 Click **Go**.

The Device and Version dialog box appears.

Step 4 Select the required device for which you wish to check the syntax using Device Selector.

Step 5 Select the information required to open a configuration file.

Field	Description
Version	
Latest	Select the latest version of the configuration file.
Earlier	Select an earlier version of the configuration file.
Version Number	Version number of the configuration file. This option is enabled when you select **Earlier** in the version field. This field is not editable. To enter the version number: 1. Click **Select** to open the Version Tree dialog box. 2. Select the desired version. 3. Either: – Click **OK** to select the version Or – Click **Cancel** to close the window.

Step 6 Click **Edit** to edit a configuration file

The Configuration Editor dialog box appears.

Step 7 Click **Tools.**

The Select Tool dialog box appears with the tools.

Step 8 Select **External Syntax Checker**.

Step 9 Click **Submit** to launch the tool.

Config Editor launches the External Syntax Checker URL.

Registering an External Syntax Checker Application With CMIC

Use CiscoWorks LMS Portal home page to register any External Syntax Checker Application.

To register an external syntax checker application with CMIC:

Step 1 Go to the CiscoWorks LMS Portal homepage and select **Common Services > Homepage > Link Registration**.

The Registered Links window appears.

Step 2 Click **Registration** in the Links Registrations Status page.

The Enter Link Attributes window appears.

Step 3 Enter the inputs for the following fields:

Field	User Notes
Name	Enter Config Syntax Checker.
URL	Enter the External Syntax Checker URL.
Display Location	Select Third Party.

The Registered Links window appears with the list of registered links.

Viewing the List of Modified Configs

You can use this feature to display a list of modified configuration files by all users in private work area (select **Private Configs**) or public work area (select **User Archive**).

To list out all the modified files:

Step 1 Select **RME > Config Mgmt > Config Editor > Private Configs** to open a configuration file stored in private work area.

The List of Private Configs window appears.

Or

Select **RME > Config Mgmt > Config Editor > User Archive** to open a configuration file stored in public work area.

The User Archived Configs window appears.

You can also perform any of the editor operations by opening a configuration file for editing by Device and Version, Pattern Search, Baseline and External Location.

For more details see, Overview: Opening a Configuration File.

Step 2 Do any of the following:

- Select the file and click **Edit** to edit an opened configuration file.

  The Configuration Editor dialog box appears.

- Select the file and click **Deploy to** deploy a job.

  The Select Configs dialog box appears.

- Select the file and click **Delete** to remove an opened configuration file.

  The screen is refreshed and the file is removed.

You can open a raw config in processed format. However, you cannot open a processed config in raw format.

Overview: Opening a Configuration File

You can use this feature to open a configuration file for editing.

You can open a configuration file by:

- Device and Version—Opens a configuration file from the archive.
- Pattern Search—Opens a configuration file by searching for a pattern.
- Baseline—Opens a configuration file using a baseline template stored in the device configuration management repository.
- External Location—Opens a configuration file stored in an external location

If another user has opened the configuration file, config editor opens another copy of the file.

To open a configuration file:

Step 1 Select **RME > Config Mgmt > Config Editor> Config Files**.

Step 2 Select an option in the Selection Area page.

Step 3 Click **Go.**

The Option dialog box opens in a new window.

Opening a Configuration File - By Device and Version

You can use this feature to open a configuration file from the archive. The file opens in read-write mode according to your edit permissions.

The file appears in either a Raw or Processed mode, based on your preferences.

To open a configuration file from the archive:

Step 1 Select **RME > Config Mgmt > Config Editor> Config Files.**

Step 2 Select **Device and Version** in the Selection Area page.

Step 3 Click **Go**.

The Device and Version dialog box appears.

Step 4 Select the required device using the Device Selector.

Step 5 Select the information required to open a configuration file.

Field	Description
Version	
Latest	Select the latest version of the configuration file.
Other	Select an earlier version of the configuration file.

Field	Description
Version Number	Version number of the configuration file. This option is enabled when you select **Other** in the version field. This field is not editable. To enter the version number: 1. Click **Select** to open the Version Tree dialog box. 2. Select the version you need. 3. Either: • Click **OK** to select the version Or • Click **Cancel** to close the window.
Format	
Raw	Displays the entire configuration file. After you open a file in a specific mode, you can view it only in that mode.
Processed	Displays only the commands.

Step 6 Click either:

- **Edit** to edit a configuration file

  The configuration editor dialog box appears.

  Or

- **Reset** to clear all fields and get to the default setting.

Opening a Configuration File - By Pattern Search

You can use this feature to open a configuration file by

- Selecting a label set in Config Archive
- Selecting a custom query of default patterns
- Searching for a pattern.

A pattern can be any text string. The file is displayed in either a Raw or Processed mode, based on your preferences.

To open a configuration file:

Step 1 Select **RME > Config Mgmt > Config Editor> Config Files**.

Step 2 Select **Pattern Search** in the Selection Area page.

Step 3 Click **Go**.

The Pattern Search dialog box appears.

Step 4 Do any of the following:

- Open a configuration file by selecting a label set in Config Archive

- Open a configuration file by selecting a custom query of default pattern
- Open a configuration file by searching for a pattern

Open a configuration file by selecting a label set in Config Archive

a. Select **Label** to enable the Select a Config Label drop-down list box

b. Select the required label from the Select a Config Label drop-down list box

Open a configuration file by selecting a custom query of default pattern

Select the required **Custom Query** from the Select Custom Query drop-down list box.

Open a configuration file by searching for a pattern

a. Enter a pattern in the editable Pattern Column. For example, *http server.*

To search for more than one pattern, enter the second and third patterns in the Pattern 2 and Pattern 3 fields and so on. You cannot search for special characters, for example, control-C.

b. Click the corresponding Contains/Does not contain row to view the selection drop-down list box.

c. Select **Include** if you wish to search for configurations that match the patterns you entered and select **Exclude** if you wish to search for configurations that do *not* match the patterns you entered.Select the required devices using the Device Selector.

Step 5 Select the required options:

Field	Description
Setting	
Match Any	Searches for configurations that have at least one of the patterns you entered.
Match All	Searches for configurations that include all patterns you entered.
Match Case	Searches for configurations that are identical to the pattern entered.
Search Version(s)	
Latest	Searches in the latest version of the configuration file
All	Searches in all the versions of the configuration file

Step 6 Click **Next**

The Search Archive Result window appears in the Pattern Search Results page with the search results. The columns in this window are:

Column	Description
Device Name	Name of the device
Version	Version of the configuration file
Created On	Date on which the configuration file is created
Change Description	Modification comments

Step 7 Select any of the following:

- **Edit** to open the selected configuration file in a pop up window for editing. The search result page will be retained. You can select some other configuration from the search result page and open that for editing.

- **Back** to return to the Pattern Search page.
- **Finish** to complete the search.
- **Cancel** to return to the Selection Criteria page.

Opening a Configuration File - By Baseline

You can use this feature to open a baseline configuration template maintained in the configuration archive. You can create a baseline configuration from the baseline template by replacing all the variables that appear in the configuration.

Config Editor does not check whether you have changed the template variables.

Note The baseline template will be opened only in Raw format.

To open a baseline configuration template:

Step 1 Select **RME > Config Mgmt > Config Editor> Config Files**.

Step 2 Select **Baseline** in the Selection Area page.

Step 3 Click **Go**.

The Baseline Config dialog box appears.

Step 4 Select the required devices using the Device Selector.

Step 5 Click **Next**

The Baseline Template window appears with the following details:

Column	Description
Baseline Name	Name of the Baseline template.
Description	Brief description about the template.
Created On	Date on which the template was created.

Step 6 Select a Baseline template based on the device type.

Step 7 Select any of the following:

- **Back** to return to the Baseline Config page.
- **Finish** to associate the selected template to a device.
- **Cancel** to return to the Selection Criteria page.

While editing baseline template, you are required to replace variables that appear in the template with actual values.

```
For example, in the following line [msg] is the variable.
banner motd [msg]
```

You should replace `[msg]` with actual value.

Baseline Configuration Editor

You can use this feature to edit the Baseline template of the configuration file.To do this:

Step 1 Select **RME > Config Mgmt > Config Editor> Config Files**.

Step 2 Select **Baseline** in the Selection Area page.

Step 3 Click **Go**.

The Baseline Config dialog box appears.

Step 4 Select the required devices using the Device Selector.

Step 5 Click **Next**.

The Baseline Template window appears with the following details:

Column	Description
Baseline Name	Name of the Baseline template.
Description	Brief description about the template.
Created On	Date on which the template was created.

Step 6 Select a Baseline template based on the device type.

Step 7 Click **Finish**.

The Baseline Configuration Editor dialog box appears.

Step 8 Edit the text area. (The upper section contains only non-credential commands and is called the text area.)

Step 9 .Enter comments for change in baseline in the Change Description field.

Step 10 Select any of the following:

- **Save** to save changes to the configuration file.
- **Undo All** to undo editing or typing changes.
- **Replace All** to replace a string in the opened configuration files.
- **Tools...** to launch the Config Editor tools.
- **Close** to close the Config Editor window.

Opening an External Configuration File

You can use this feature to associate a device with the selected configuration file from an external location (other than archive) in the server. The file appears in either a Raw or Processed mode, based on your preferences.

For example, if you associate the selected configuration to an IOS device in the Processed mode, then the given configuration is processed based on the IOS rules defined in RME.

The file in the archive can be opened with a specified format from the temp directory on the local server or from another file system mapped drive or any mount. The file opened is validated for format with DCMA.

To open a configuration file from an external location:

Step 1 Select **RME > Config Mgmt > Config Editor > Config Files**.

Step 2 Select **External Location** in the Selection Area page.

Step 3 Click **Go**.

The External File Selection dialog box appears.

Step 4 Click **Browse** to select the external file location.

The External Config Selector dialog box appears with the following fields:

Field	Description	Usage Notes
File	Location of the file	Enter the file location. For example, D:/CSCOpx
Directory content	Name of the directory	Select the directory. For example, bin/
Drive	Name of the drive	Select the drive. For example, D:\

Step 5 Click either:

- **OK** to enter the external location.

  Or

- **Cancel** to return to the External File Selection page.

Step 6 Select the required devices using the Device Selector.

Step 7 Either:

- Click **Edit** to edit a configuration file

  The configuration editor dialog box appears.

  Or

- Click **Reset** to clear all fields and get to the default setting.

You can control the access to directories/folders present on the server. There is a property file for this purpose:

NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/config/cfgedit/ConfigEditor.properties.

This file has two variables:

- *DIR_LIST*—You can mention all the directories or files separated by pipe symbol (|).
- *ALLOW*—You can be set as true or false. If you set the value as true, means you can access only those directories or files given as values for the variable *DIR_LIST*. If you set the value as false, you cannot access those directories or files given as values for the variable *DIR_LIST*.

The default values for the variables are:

- *DIR_LIST*—`etc/passwd`

- *ALLOW*—`false`

What Happens During Configuration Deployment in Overwrite and Merge Modes

Overwrite Mode

Config Editor assumes that the latest archived version is the same as the running configuration on the device.

Before Config Editor downloads the archived configuration on the device, it compares the archived version (which you have modified) with the latest version. The application then overwrites the running configuration on the device with the archived version. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same.

For example, assume that the archived version contains commands a, b, c, and d; and that the latest running version, contains commands a, b, e, f, and g. After the archived configuration has been restored, the currently running configuration on the device, will contain commands a, b, c, and d.

Ensure that all the required commands are in the archived version. You can review the work order and make necessary changes by editing the archived version, if required.

This is the default mode for the configuration deployment.

Merge Mode

The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration.

The selected running configuration is not compared with the running configuration in the Configuration Archive.

We recommend that you use this mode on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device.

Overview: Downloading a Configuration File

To download a configuration file to the device and to the archive, you must:

- Start creating a download job.
- Select the configuration file on which the job will run.
- Configure the job properties.
- Set the job approvers.
- Review the job work order.

When a job starts to download, the users on the job approver list are notified by e-mail. At least one approver must approve the job before it can run. Make sure that an approver list with the approvers you want exists.

If there is no approver list but you have the correct access privileges, you must modify or create approver lists, using the Job Approval option (Select **RME> Admin> Approval**). Otherwise, contact your system administrator.

Starting a New Download Job

You can use the Create Config Download Job wizard to define and schedule a download job.

Step 1 Select **RME > Config Mgmt > Config Editor > Config Editor Jobs**.

The Config Deploy Job Browser window appears.

Step 2 Click **Create**.

The Create Config Download Job wizard appears.

All dialog boxes of the wizard contain the following buttons:

Button	Description
Back	Returns to the previous page.
Next	Returns to the next page.
Finish	Completes creation of jobs.
Cancel	Cancels creation of job.

Selecting Configs

You can use the Select Configs dialog box to select configuration files of devices on which the download job will run.

You must start a new download job before you start selecting configuration files. To do this:

Step 1 Select a configuration file on which to run the job using device selector on the left pane.

The select configuration file dialog has two panes.

- Left Pane—The Device Selector appears.
- Right Pane—The list of selected configuration files appear.

Step 2 Click either:

- **Add Latest** to move the latest version of the selected configuration file to the Selected Configuration File(s) pane

  Or

- **Add Other Version** to move any version of the selected configuration file to the Selected Configuration File(s) pane

Step 3 Do any of the following:

- Click **Next** to proceed to the Job Schedule and Options dialog box.
- Click **Cancel** to stop creating a download job.

- Select a configuration file from the Selected Configuration File(s) pane and Click **Delete** to remove a configuration file.

Scheduling a Job

This feature allows you to assign a job name, schedule the job and set job options.

Before scheduling a job you must:

1. Start a new download job.
2. Select Configs.

To schedule a job:

Step 1 Enter the following information in the Job Schedule and Options dialog box.

Field	Description/Action	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future. Select either Once or Immediately.	You can specify when you want to run the job. To define this, select an option from the drop down menu: Once—Job will run once in the future. You can specify the Starting Date and Time for the job to be run Immediately—Job will run immediately. This option is not available if Job Approval is enabled.
Date	Date on which you want to run the job.	Select date for the job to run. If Run Type is Immediate, the system date is automatically selected.
At	Time when you want to run the job in the future.	Select time for the job to run. If Run Type is Immediate, the system time is automatically selected.
Job Info		
Job Description	Enter job description.	Make each description unique so you can easily identify jobs.
E-mail	Allows you to enter the e-mail addresses to which the job will send status notices. Separate multiple addresses with commas.	E-mail notification is sent when job is created, started, deleted, canceled, and completed.
Comments	Allows you to enter comments.	
Approval Comment	Allows you to enter approval comments.	This field is not active if approval comments were not set using RME administration approval. Select RME > Admin > Approval to set approval comments. For more information, see Approving and Rejecting Jobs Online help.

Field	Description/Action	Usage Notes
Maker E-mail	Mail ID of the person who created the job.	This field is not active if approvers were not set using RME administration approval. Select RME > Admin > Approval to set approval comments. For more information, see Approving and Rejecting Jobs Online help.

Field	Description/Action	Usage Notes
Job Options		
Fail on mismatch of Configuration Version	Select this option, if you want to cause the job to be considered Failed, if there is a version mismatch.	A job is considered Failed when the most recent configuration version in the configuration archive is not identical to the configuration that was running when you created the job.
Sync archive before executing a job	Select this option if you want to archive the running configuration before making configuration changes.	Synchronize archive before executing a job policy gets selected when Fail on mismatch of Configuration Version policy is selected.
Delete Config after Download	Select this option if you want to delete the configuration file after download.	Applicable only to private configuration files.
Copy running to Startup	Select this option if you want to copy the running configuration to the startup configuration on each device after configuration changes are made successfully.	This does not apply to Catalyst OS devices.
Enable Job Password	Select this option to enable username and password.	
User Name	Enter the username configured on the device.	This field is editable only when you select the Enable Job Password option. Resource Manager Essentials (RME) ignores the username in the RME database and uses the newly entered username instead.
Password	Enter the password for the device.	This field is editable only when you select the Enable Job Password option. Resource Manager Essentials (RME) ignores the password in the RME database and uses the newly entered password instead.
Enable User Name	Enter the name of the enable user configured on the device.	This field is editable only when you select the Enable Job Password option. Resource Manager Essentials (RME) ignores the password in the RME database and uses the newly entered password instead.
Enable Password	Enter the enable password configured on the device.	This field is editable only when you select the Enable Job Password option. Resource Manager Essentials (RME) ignores the password in the RME database and uses the newly entered password instead.

Field	Description/Action	Usage Notes
Failure Policy	Specify what the job should do if it fails to run on the device.	• Select **Ignore Failure and Continue** from the drop-down list box to continue the job and make configuration changes to the remaining devices, configured by the job Or • Select **Stop on Failure** to stop making changes to the remaining devices.
Execution	Mode in which the job is executed. There are two options, Parallel and Sequential.	1. Select **Parallel** to run the job on multiple devices at same time Or Select **Sequential** to run the job one device at a time. 2. Click **Device Order.** The Set Device Order dialog box appears. 3. Use the Up and Down arrows to move a device up or down. 4. Click **Done**.
Download Mode	Mode in which the configuration file is downloaded. The two modes are Overwrite and Merge.	Do either of the following: • Select the **Overwrite** option, if you want to replace the existing running configuration on the device, with the selected configuration. This is the default option for the configuration deployment. The configuration that you have selected is compared with the latest running configuration in the Configuration Archive. (RME assumes that the latest running configuration in the archive is the same as the configuration currently running on the device.) The Overwrite mode ensures that the running configuration on the device is overwritten with the selected configuration. This means, after the configuration is successfully deployed, the selected configuration and the running configuration on the device are the same. Overwrite mode supports only Write2Run of the configuration. Or • Select the **Merge** option, if you want to add incremental configuration to the device. The configuration that you have selected is deployed on to the device as is. This means, the existing running configuration of the device is updated incrementally with the commands in the selected configuration. The selected running configuration is not compared with the running configuration in the Configuration Archive. We recommend that you use this option on newly deployed devices. This is because, the Merge option effectively deploys the entire configuration from the archive, on to the device. Merge mode supports both Write2Run and Write2Start of the configuration.

Field	Description/Action	Usage Notes
Push Config to	The method in which the Configuration is pushed. The two methods are Running and Startup	Do either of the following: Select the **Running** option, if you want to replace the existing running configuration on the device, with the selected configuration file. This is also referred to as Write2Run. Or Select the **Startup** option, if you want to erase the contents of the device's startup configuration and write the contents of the given file as the device's new startup configuration. This is also referred to as Write2Start. Configurations edited from Raw mode (.RAW) can be downloaded to both Startup or Running configuration of the device. Configurations edited from Processed mode (.PROC) can only be downloaded to the Running configuration of the device.
Update RME credentials after deploy	Update the credentials in DCR after deployment, if the deployed commands include any credentials commands.	Choose this option if you want to update the DCR with the deployed credentials commands such as SNMP community strings, Telnet username/password etc. Write2Start does not support changing the RME credentials after deployment.

Step 2 Select any of the following:

- **Back** to return to the Select Configs dialog box.
- **Next** to proceed to the Job Summary dialog box.
- **Cancel** to stop creating a Download job.

Configuring Job Policies for Config Editor

You can configure a default policy for job properties that applies to all future jobs.

You can also specify if the property can be modified when the job is created.

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To do this:

Step 1 Select **RME > Admin > Config Mgmt > Config Job Policies**.

The Config Job Policies dialog box appears.

Step 2 Select **Config Editor** from the application drop-down list.

Step 3 Enter the following information in Config Job Policies dialog box.

Field Name	Description	Usage Notes
Failure Policy This appears only if you select either Config Editor or NetConfig application.	Specify what the job should do if it fails to run on the device. You can stop or continue job, and roll back configuration changes to failed device or all devices configured by the job. You can select one of the options: • Stop on failure—Stops the job on failure. • Ignore failure and continue—Continues the job on failure. • Rollback device and stop—Rolls back the changes on the failed device and stops the job. This is applicable only to NetConfig application. • Rollback device and continue—Rolls back the changes on the failed device and continues the job. This is applicable only to NetConfig application. • Rollback job on failure—Rolls back the changes on all devices and stops the job. This is applicable only to NetConfig application.	You can create rollback commands for a job in the following ways: • Using a system-defined template. Rollback commands are created automatically by the template. The Banner system-defined template does not support rollback. You cannot create rollback commands using this template. • Creating a user template. Allows you to enter rollback commands into the template. When you use the Adhoc and Telnet Password templates, you cannot create rollback commands.
E-mail Notification This appears for all the applications in the dropdown list.	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.	Notification is sent when job is started and completed. Notification e-mails include a URL to enter to display job details. If you are not logged in, log in using login panel.
Sync Archive before Job Execution This appears if you select either Config Editor or NetConfig application.	The job archives the running configuration before making configuration changes.	None.
Copy Running Config to Startup This appears if you select either Config Editor or NetConfig application.	The job writes the running configuration to the startup configuration on each device after configuration changes are made successfully.	Does not apply to Catalyst OS devices.

Field Name	Description	Usage Notes
Enable Job Password This appears for all the applications in the dropdown list.	The Job Password Policy is enabled for all the jobs. The Archive Management, Config Editor, and NetConfig jobs use this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository. These device credentials are entered while scheduling a job.	None.
Fail on Mismatch of Config Versions This appears if you select either the Config Editor or NetConfig application.	The job will be considered a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job.	None.
Delete Config after download This appears if you select Config Editor.	The configuration file is deleted after the download.	
Execution Policy This appears for all the applications in the dropdown list.	Allows you to configure the job to run on multiple devices at the same time (Parallel execution) or in sequence (Sequential Execution).	If you select Sequential execution, you can click Device Order in the Job Schedule and Options dialog box to set the order of the job. **1.** Select a device in the Set Device Order dialog box. **2.** Either: • Click the Move Up or Move Down arrows to change its place in the order. Click **Done** to save the current order. Or • Close the dialog box without making any changes.
User Configurable	Select this check box next to any field to make corresponding policy user configurable.	You can configure a user-configurable policy while defining job. You cannot modify non-user-configurable policies.

Reviewing the Work Order

The work order summarizes the job you created. If you find any changes missing when you review the work order you can go back and change the options.

Complete the following prerequisite steps of the job definition process:

1. Start a new download job.
2. Select configs.
3. Configure job properties.
4. Set job approvers, if Job Approval is enabled.

To review the work order:

Step 1 Review the information in the Work Order dialog box.

The fields in this dialog box are:

Field	Description
General Info	Detailed information about the job, such as owner, description and schedule.
Job Approval Info	Status of approval.
Job Policies	Policies configured for the job. Edit in Job Properties dialog box.
Devices	Devices on which the job will run. Edit in Device Selector dialog box.
Device Commands	Commands that the job will run.
Username	Username of the job owner.

- To modify the job, return to any previous dialog box and change the information.
- To return to a previous dialog box, click **Back** until the dialog box appears.

Step 2 Click **Finish** in the Work Order dialog box to register the job.

Viewing the Status of all Deployed Jobs

You can use this feature to view the status of all pending, running, and completed jobs. You can create a new job or edit, copy, stop and delete a job that you have opened.

You can only Edit one job at a time while you can Stop or Delete multiple jobs at a time.

To view all the downloaded jobs:

Step 1 Select **RME > Config Mgmt > Config Editor > Config Editor Jobs**.

The List of Deploy Jobs window appears with the list of all the jobs.

Column	Description
Job ID	Unique number assigned to job at creation. Never reused.
Run Status	Job states: • Canceled, • Suspended, • Missed start, • Rejected, • Succeeded, • Succeeded with info, • Failed, Crashed, • Failed at start, • Running.
Description	Description of the job, as entered during job definition.
Owner	Name of the user who owns the configuration file.
Scheduled On	Date and time the job is scheduled to run.
Completed At	Date and time at which the job is completed.
Schedule Type	Job schedule types: • Suspended, • Scheduled, • Waiting for approval, • Rejected, • Canceled.
Status	Status of running or completed jobs: Job Started, Progress, Job Cancelled, Job Failed, Job Successful. Pending jobs have no status.

Step 2 Click one of the following buttons:

Button	Description	Usage Notes
Create	Creates a new job.	1. Click **Create**. The Create Config Deploy Job wizard appears. 2. Use the wizard to define and schedule a download job.
Edit	Edits pending job. The Job definition opens with the current information, including Job ID. You can edit the job in the same way as you can define and schedule a new job.	Click **Edit** to edit only jobs you own. If the job start time occurs during editing, it will run without the edits. In such a case, you can complete your edits, reschedule the job, and re-edit it. To prevent job from running unedited: 1. Complete edits before job start time. 2. Cancel job and create new one.
Copy	Copies job. You can edit the job in the same way as you can define and schedule a new job.	Click **Copy**. The Job definition opens with the current information and the new ID except job schedule details filled in.
Stop	Stops a running job.	1. Click **Stop**. You are prompted to confirm stopping a job. 2. Click **OK.** You can stop only the jobs that you own. Admin level users can stop all jobs.
Delete	Removes the job from the Job Scheduler.	1. Click **Delete**. You are prompted to confirm stopping a job. 2. Click **OK** or **Cancel**. You can remove only the jobs that you own. Admin level users can remove all jobs.

CHAPTER 11

Using NetShow Commands

Network show (NetShow) commands represent a set of read-only commands. These are primarily, `show` commands that you can run on devices that are managed in RME.

You can specify the commands that you want to group together and then run these commands on one or many devices. The output is displayed in a browser window.

NetShow has the following features:

- Network Administrators can assign Command Sets to other users.
- Network Administrators and Network Operators (if permitted) can execute the custom commands. This allows them to run a command against multiple devices.
- Support for standard and non-standard Cisco devices.
- Simplified new device support.
- No device limit.
- Integration with the Output Interpreter tool.

RME ships with system-defined NetShow Command Sets. You cannot edit or delete any of these Command Sets. See System-Defined Command Sets for the list of system-defined Command Sets in RME.

You can run NetShow commands either from the Graphical User Interface (GUI) or from the Command Line Interface (CLI). NetShow allows you to add system-defined as well as adhoc commands within Command Sets and run them.

You must have the required privileges to perform these functions. See Viewing the Permission Report for the tasks that a user in a particular role can perform.

The major features of NetShow are:

- NetShow Job Browser

  The NetShow job browser allows you to create, edit, copy, retry, stop, or delete NetShow jobs and view the details of the jobs. You can run a job immediately or schedule it to run at a specified time, once, or periodically.

- Archiving NetShow Job Output

  You can access the stored output that is created from a NetShow job through the Output Archive.

- Command Sets

  The Command Set administration task enables you to create, edit, or delete user-defined Command Sets.You can also view the details of existing Command Sets.

- Assigning Command Sets

Allows you to assign Command Sets to users. You can assign one or more Command Sets and Custom Command Execution privilege to one or more users.

Working With NetShow Jobs

The NetShow Jobs feature allows the user with appropriate privileges to perform tasks such as viewing job details, creating jobs, editing jobs, copying jobs, retrying failed jobs, stopping jobs, and deleting jobs.

For a list of NetShow Job tasks and the required user roles, use the Permission Report function (**Common Services > Server > Reports**). See Viewing the Permission Report for more details.

Viewing the Permission Report

The Permission Report displays information on roles and tasks associated with the roles. It specifies the tasks that a user in a particular role can perform.

To use CiscoWorks, you must have a valid login, which is a combination of a username and a password.

When you are assigned a username and password, you are also assigned to one or more of these roles:

- Help Desk (default role for all users) —Can access network status information only. Can access persisted data on the system but cannot perform any action on a device or schedule a job which will reach the network.
- Approver— Can approve all tasks.
- Network Operator— Can perform all Help Desk tasks. Can perform tasks related to network data collection but not any task that requires write access on the network.
- Network Administrator —Can perform all Network Operator tasks. Can perform tasks that result in a network configuration change.
- System Administrator —Can perform all CiscoWorks system administration tasks.

These roles determine which CiscoWorks applications, tools, and product features you are allowed to access.

Roles are not set up hierarchically, with each role including all the privileges of the corresponding role. Instead, these roles provide access privileges based on user needs.

To view the roles and corresponding tasks that these roles can perform in NetShow:

Step 1 Select **Common Services > Server > Reports > Permission Report > Generate Report**.

The Permission Report appears.

Step 2 Check the Permission Report to verify which of the NetShow tasks each user role can perform.

The following table lists the NetShow tasks that each user role can perform.

Task Name	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Assign Command Sets to Users	No	Yes	No	No	No
Create, Edit, Cancel, Delete Jobs	No	Yes	Yes	No	No

Task Name	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Create, Edit, Delete Command Sets	No	Yes	Yes	No	No
Job Browser	No	Yes	Yes	Yes	No
View Command Sets	No	Yes	Yes	No	No

By default, System-defined Command Sets are assigned to Network Administrators and Network Operators.

Only Network Administrators can assign Command Sets to Network Operators. They can also view Command Sets created by all users.

Network Operators can create and view Command Sets for themselves. These Command Sets will be automatically assigned to them. However, they cannot view Command Sets created by other Network Operators.

NetShow Job Browser

The NetShow Job Browser enables you to view the details of all NetShow Jobs. The job details that you can view are:

- Job ID
- Job status
- Job description
- Job owner
- Time the job is scheduled to run at
- Time the job completes
- Schedule type

To use the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears.

You can filter the jobs by any specified criteria using the Filter by drop-down list.

Step 2 Select your criteria and click **Filter**.

The fields in the NetShow Job Browser are:

Column	Description
Job ID	Unique ID of the job. Click the hyperlink to view the Job details. For periodic jobs, the Job IDs are in the *number.x* format, which stands for the number of instances of that job. For example, 1003.3 indicates that the Job ID is 1003 and it is the third instance of that job.
Status	Status of the job—Scheduled, Successful, Failed, Cancelled, Running, Missed Start, Rejected, Approved, Waiting for Approval. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. This count of failed devices is not displayed for jobs restored from RME 4.0.4 or lesser versions.
Description	Description of the job.
Owner	Username of the job creator.
Scheduled At	Date and time at which the job was scheduled.
Completed At	Date and time at which the job was completed.
Schedule Type	Type of job schedule—Immediate, Once, 6- Hourly, 12-Hourly, Daily, Weekly, Monthly, Last Day of the Month. For periodic jobs, the subsequent instances will run only after the earlier instance of the job has completed. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.

Refresh (Icon)	Click this icon to refresh the NetShow Job Browser.

The NetShow Job Browser allows you to perform the following tasks:

- Viewing Job Details
- Creating Jobs
- Editing Jobs
- Copying Jobs
- Retrying Jobs
- Stopping Jobs
- Deleting Jobs

Viewing Job Details

From the NetShow Job Browser, you can select a job and view its details.

To view the Job Details:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears.

Step 2 Click the Job ID hyperlink of the job whose details you want to see.

The NetShow Job Details pop-up appears, displaying the day, date and time details in the header at the top of the page. The Job ID and the Status appear in the header of the Job Result.

By default, the NetShow Job Details page appears with the Job Details list tree in the left pane and the Work Order, in the right pane.

The Job Details list tree contains the following:

- Job Summary—Displays the summary of the job.
- Device Details—Displays the status of the devices.
- Work Order—Displays the work order of the job.

The following table describes the Job Details page.

Page/Folder	Description	
Job Details	Job Summary	Click to display summary of completed job: • Deploy Summary: – Status – Start Time – End Time • Job Messages – Pre-job Execution – Post-job Execution • Device Update – Successful – Failed – Not Attempted – Pending

Page/Folder	**Description**	
Device Details	Deployed Devices	Contains detailed job results for each device in a table: • Device—List of devices on which the job ran. • Status—Status of the device deployment (success or failure.) • Protocol Used—Protocol used for the device. • Message – If the job failed on the device, the reason for failure appears. – If the job succeeded on that device, the message `Deploy Successful` appears. You can filter the devices by selecting a status and clicking **Filter**. This page displays the number of rows you have set for display in the Rows per page field. You can increase the rows up to 50 on each page. You can navigate between the pages of the report using the navigation icons at the right bottom of this table. Click the device name link to view the details of command sets and commands on the device. Go to Step 3 for details. You can view the output of all the commands for all the devices by clicking the **Print** button on the top right hand corner of the NetShow Job Details Page.
	Pending Devices	Displays the list of devices that are awaiting command deployment.
	Not Attempted Devices	Displays the list of devices on which the job has not attempted to deploy commands.
Work Order	Displays the Job Work Order. It contains the same information as the work order that appeared when the job was created. For retried jobs, job definitions are not updated. For such jobs the original job definitions are retained. See A sample Job Work Order is: for details.	

You can click the page icon in the left pane to get the corresponding results in the right pane.

Step 3 Click the device name link in the Device Details table.

The NetShow Device Details pop-up page appears with the device name and commands in the left pane and the commands output in the right pane.

By default, the command output is a consolidated one for all the listed commands.

To convert the output into a printer-friendly format click the **Printer** button.

A printer-friendly format of the consolidated output for all commands appears.

Step 4 Select a command from the Device list tree in the left pane and click **Analyze Output** to analyze the output of the command.

You can mask the credentials shown in the output of **`show`** commands. See Masking Credentials for more details on masking credentials and Viewing and Analyzing NetShow Output for more details on viewing and analyzing NetShow Output.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

Step 5 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credential Profile dialog box

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Step 6 Click **OK** after entering the credential information.

The credentials that you enter here will be used for the entire session.

The Show Commands Output Interpreter Viewer appears, displaying the Report Name, date and time details in the header at the top of the report.

To convert the output into a printer-friendly format click the **Printer** button.

A printer-friendly format of the output of the selected command appears.

Masking Credentials

You can mask the credentials shown in the output of **`show`** commands. If you want to mask the credentials of a particular command, you must specify the command in the *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\config\netshow\NSCredCmds.properties file.

In this file you can specify all the commands whose output should be processed to mask the credentials. We recommend that you enter the complete command in the file. For example, you must enter **`show running-config`**, not
`show run.` This file contains some default commands like **`show running-config`**.

Creating Jobs

From the NetShow Job Browser, you can create new jobs to run command sets. You can create immediate as well as scheduled jobs.

To create a new job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears.

Step 2 Click **Create** in the NetShow Job Browser.

The Select Devices and Command Sets window appears.

Step 3 Select the device or Device Categories from the Device Selector pane in the Select Devices and Command Sets window.

Step 4 Select the Command Set from the Command Set List pane in the Select Devices and Command Sets window.

Step 5 Enter the custom commands in the Custom Commands text box.

You can enter multiple commands; separate these commands by commas.

The Custom Commands text box will be enabled only if you have custom commands execution privilege. See Assigning Custom Command Execution Privilege for more details on assigning custom command execution privilege.

Step 6 Click **Next**.

The Set Schedule Options dialog box appears.

Step 7 Enter the following information in the Set Schedule Options dialog box:

Field	Description
Scheduling	
Run Type	The run type of the job. The Run Types could be any or all of these, depending on the type of the job: • Immediate—Runs the job immediately. • Once—Once at the specified date and time. • 6 -hourly—Every 6 hours, starting from the specified time. • 12 -hourly—Every 12 hours, starting from the specified time. • Daily—Daily at the specified time. • Weekly—Weekly on the day of the week and at the specified time. • Monthly—Monthly on the day of the month and at the specified time. • Last day of Month—On the last day of the month at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	Scheduled date and time of the job.
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter your comments for the job. Comments appear in the Job Work Order.

Field	Description
Job Options	
Enable Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and Device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and Device Enable password. The credentials are for contacting the device and not the DCR credentials. Or – Disable the Job Password option in the Set Schedule Options dialog box.
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple (up to five) devices at the same time. • Sequential—Allows the job to run on only one device at a time.
Maker Comments	This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments. See Setting Up Job Approval for more details on enabling Job Approval Policies.
Maker E-mail	This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory. See Setting Up Job Approval for more details on enabling Job Approval Policies.

Step 8 Click **Next**.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

- Job policies.
- Job approval details (if you have enabled job approval).
- Device details.
- Command Sets and the commands to be executed.

Step 9 Click **Finish** after you review the details of your job in the Job Work Order.

A message appears, `Job ID created successfully`.

The newly created job appears in the NetShow Job Browser.

If your job failed and you want to run the same job, click **Retry** and perform steps **7** through **9** above.

A sample Job Work Order is:

```
-----------------------------------------------------------------
Work Order

Name: NetShow Job Work Order

Summary: General Info
```

```
--------------------------------------------------------------
Job Id: 1018
Owner: admin
Description: cli scheduled
Schedule Type: Run Once
Schedule Time: Sat Mar 19 00:00:00 IST 2005

-----------------------------------------------------------------
Job Policies

E-mail Notification: Disabled
Execution Policy: Parallel
Job Password: Disabled

---------------------------------------------------------
Job Approval Details

Job Approval: Disabled
--------------------------------------------------------

Device Details

Device: 10.76.38.14
Applicable Commands:
Command Set Name: Show System Info
show version
show flash
show logging



ADHOC Commands
sh ver
------------------------------------------------------------------
```

Editing Jobs

You can select a job and edit the job properties from the NetShow Job Browser. You can edit only the scheduled jobs.

You can change device and command set selection as required and re-submit the job. In such cases the Job ID will remain the same.

To edit a job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears with a list of all jobs.

Step 2 Select a scheduled job and click **Edit** in the NetShow Job Browser.

The Select Devices and Command Sets window appears with the current settings.

Step 3 Select the device or Device Categories from the Device Selector pane in the Select Devices and Command Sets window.

Step 4 Select the Command Set from the Command Set List pane in the Select Devices and Command Sets window.

Step 5 Enter the custom commands in the Custom Commands text box.

You can enter multiple commands. Separate these commands by commas.

The Custom Commands text box will be enabled only if you have custom commands execution privilege. See Assigning Custom Command Execution Privilege for more details on assigning custom command execution privilege.

Step 6 Click **Next**.

The Set Schedule Options dialog box appears.

Step 7 Enter the following information in the Set Schedule Options dialog box:

Field	Description
Scheduling	
Run Type	The run type of the job. The Run Types could be any or all of these, depending on the type of the job: • Immediate—Runs the job immediately. • Once—Once at the specified date and time. • 6 -hourly—Every 6 hours, starting from the specified time. • 12 -hourly—Every 12 hours, starting from the specified time. • Daily—Daily at the specified time. • Weekly—Weekly on the day of the week and at the specified time. • Monthly—Monthly on the day of the month and at the specified time. • Last day of Month—On the last day of the month at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	Scheduled date and time of the job.
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.

Field	Description
E-mail	Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter your comments for the job. Comments appear in the Job Work Order.
Job Options	
Enable Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and Device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and Device Enable password. The credentials are for contacting the device and not the DCR credentials. Or – Disable the Job Password option in the Job Schedule and Options dialog box.
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple devices at the same time. You can run the job on five devices at a time. • Sequential—Allows the job to run on only one device at a time.
MakerComments	This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments. See Setting Up Job Approval for more details on enabling Job Approval Policies.
Maker E-mail	This field appears if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory. See Setting Up Job Approval for more details on enabling Job Approval Policies.

Step 8 Click **Next**.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

- Job policies.
- Job approval details (if you have enabled job approval).
- Device details.
- Command Sets and the commands to be executed.

Step 9 Click **Finish** after you review the details of your job in the Job Work Order.

A message appears, `Job ID edited successfully`.

The edited job appears in the NetShow Job Browser. This job retains the original Job ID.

See A sample Job Work Order is: for details.

Copying Jobs

From the Netshow Job Browser, you can select a job and create a copy of that job. You can either edit the job details or submit the same job. If you copy a job, it creates a new job with the current administrative settings.

To copy a job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears with a list of all jobs.

Step 2 Select the job you want to create a copy and click **Copy**.

The Select Devices and Command Sets window appears with all your selections for the job that you are copying.

Step 3 Click **Next**.

The Set Schedule Options dialog box appears.

Step 4 Click **Next**.

The View Job Work Order dialog box appears with the Job Work Order.

Step 5 Click **Finish**.

A message appears, `Job ID created successfully`.

The newly created job with the copied job details appears in the NetShow Job Browser.

Stopping Jobs

This topic captures procedures for stopping and retrying jobs. From the NetShow Job Browser:

- You can select jobs that are not yet executed or jobs that are currently running, and stop them. You can select only one job at a time and stop it.
- You can select failed jobs and retry them (see Retrying Jobs).

When you use this feature to stop a job, the job status changes to the Cancelled state.

To stop a job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears with a detailed list of all jobs.

Step 2 Select the job you want to stop and click **Stop**.

A message appears, `The selected job will be stopped.`

Step 3 Either:

- Click **OK** to confirm.

Or

- Click **Cancel** to prevent the job from stopping.

If you have selected a periodic job, a message appears, `Do you want to stop all the instances?`

Step 4 Either:

- Click **OK** to stop all instances of the job.

Or

- Click **Cancel** to stop only one instance of the job.

If you confirm stopping the job, a message appears, *Job ID* `is being stopped. It may take a few seconds.`

Step 5 Click **OK**.

The status of the job appears as `Cancelled` in the NetShow Job Browser.

Retrying Jobs

From the Netshow Job Browser, you can select a failed job and retry that job. You can only retry non-periodic jobs.

To retry a failed job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears with a list of all jobs.

Step 2 Select the job you want to retry and click **Retry**.

The Set Schedule Options dialog box appears.

You can either retain or change the Schedule Options.

Step 3 Click **Next**.

The View Job Work Order dialog box appears with the Job Work Order.

Step 4 Click **Finish**.

A message appears, `Job` *ID* `submitted for retry successfully`.

The job appears in the NetShow Job Browser with the same ID.

Deleting Jobs

You can delete all jobs from the Job Browser except jobs that are already running. To delete a running job, you must first stop the job.

You can also delete individual instances of periodic jobs. However, if you try to delete the scheduled instance of the periodic job, you are prompted to confirm whether you want to delete all the instances of the job. You can delete multiple jobs at the same time.

Even if you delete a job that has completed, you can view the command output in the output archive unless you remove this archive.

To delete a job from the NetShow Job Browser:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > NetShow Jobs**.

The NetShow Job Browser appears with a detailed list of all jobs.

Step 2 Select a job or a number of jobs that you want to delete and click **Delete** in the NetShow Job Browser.

A message appears, `Selected job(s) will be deleted.`

Step 3 Either:

- Click **OK** to confirm.

Or

- Click **Cancel** to prevent the job(s) from deleting.

If you have selected periodic job(s), a message appears, `If you delete periodic jobs or instances of a periodic job that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue?`

Step 4 Either:

- Click **OK** to delete all instances of the job(s).

Or

- Click **Cancel** to cancel deleting the job(s).

If you confirm deleting the job, a message appears, `Job(s) deleted successfully.`

Archiving NetShow Job Output

The Output Archive feature in NetShow helps you archive and access the stored output that is created from a NetShow job. The **`show`** command output is archived only if the jobs are executed completely.

The Output Archive Analyzer feature reads **`show`** command outputs, interprets the data and generates a report. The Output Interpreter tool in Cisco.com performs the **`show`** command analysis.

NetShow sends selected output to Cisco.com, gets the analyzed details and displays these details in a separate window. The final output is a complete analysis of the command output. The errors and potential problems are highlighted in the report.

You can analyze the complete output of a particular command on a device.

The command output displays the analyzed output generated only for a selected command. You can generate a printer-friendly format of the command output.

Viewing and Analyzing NetShow Output

You can view and analyze a NetShow Job Output.

To view and analyze the NetShow Output:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Output Archive**.

The Output Archive page appears.

You can use the Filter option to filter the archives based on All or Job ID or Description as the criteria. You can provide a search string in the text area and click **Filter** to filter the archives based on the search criteria.

Step 2 Select an Archive ID and click **View**.

The NetShow Archive Details pop-up appears, displaying the day, date, and time details in the header at the top of the page. The Archive ID appear in the header of the Archive Result.

The Archive Details pop-up has two panes. The Archive Details appear in a tree format with Device Details and Deployed Devices in the left pane. The list of devices appear in a table in the right pane.

The following table describes the Archive Details page.

Folder	Description
Archive Details	Expand the list tree to view the Device Details and Deployed Devices.
Device Details	Expand the list tree to view the Deployed Devices.
Deployed Devices	Contains detailed job results for each device in a table: • Device—List of devices on which the job ran. • Status—Status of the device deployment (success or failure.) • Protocol Used—Protocol used for the device. • Message – If the job failed on the device, the reason for failure appears. – If the job succeeded on that device, the message `Deploy Successful` appears. This page displays the number of rows you have set for display in the Rows per page field. You can increase the rows up to 50 for each page. You can navigate among the pages of the report using the navigation icons at the bottom right of this table. Click the device name link to view the details of command sets and commands on the device. Go to Step 3 for details.

Step 3 Click the device name link in the Device Details table.

The NetShow Device Details pop-up appears with the device name, Command Sets and commands in the left pane and the command output in the right pane.

By default, the command output is a consolidated output for all the commands.

To get specific outputs for each command:

a. Select a command from the Device list tree in the left pane.

b. Click **Analyze Output** to view and analyze the output of the command.

If the selected command's output appears as `No Output` in the right pane, the **Analyze Output** button is disabled.

You can mask the credentials shown in the output of **`show`** commands. See Masking Credentials for more details.

The Cisco.com Profile pop-up dialog box appears.

Step 4 Enter your Cisco.com Username and Password in the dialog box.

The credentials that you enter here will be used for the entire session.

The Show Commands Output Interpreter Viewer appears. It displays the report name, date, and time details in the header at the top of the report.

To convert the output in to a printer-friendly format click the **Printer** button.

Deleting Output Archive

You can use this feature to delete the output of a NetShow Job archive. However, this action will not delete the corresponding job details.

To delete the Output Archive:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Output Archive**.

The Output Archive page appears.

You can use the Filter option to filter the archives based on All or Job ID or Description as the criteria. You can provide a search string in the text area and click **Filter** to filter the archives based on the search criteria.

Step 2 Select the archive(s) that you want to delete and click **Delete**.

A message appears, `Selected archive(s) will be deleted`.

Step 3 Either:

- Click **OK** to delete the selected archive(s).

Or

- Click **Cancel** to cancel deleting the selected archive(s).

Command Sets

The Command Set represents a logical grouping of commands. Each command set is associated with a unique name.

NetShow provides a few pre-defined command sets that can be run against selected devices. See System-Defined Command Sets for more details on these command sets.

The command set can contain multiple commands in the following types of devices:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Routers
- Switches and Hubs
- Security and VPN

- Broadband Cable
- Storage Networking
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules

Since the command set itself contains `show` commands for different device types, you use them to run on multiple devices of various device types. You must identify the required command sets to solve a particular problem.

When you run command set on different types of devices, it sends only the `show` commands applicable for that device type. These command sets help you getting lab wide network status.

The Network Administrator and Network Operator can create command sets. The Network Administrator can assign command sets to other users.

When you migrate from RME 3.x to RME 4.x, Command Sets in RME 3.x that have special characters will not appear in the RME 4.x NetShow GUI. The valid characters for Command Set names are:
A to Z, a to z, 0 to 9, -, _, .,), (, /, and blank space.

Characters other than these are considered as special characters, and will not appear in the NetShow GUI.

System-Defined Command Sets

The following table describes the System-defined command sets in NetShow:

Command Set	**Commands**
Show Cable Hop Info	Displays cable hop statistics
Show Cable Modem Info	Displays information for the registered and unregistered CMs
Show Cable Modulation-Profile	Displays modulation profile group information
Show Cable QoS Profile Info	Displays quality-of-service (QoS) profiles
Show Cable Spectrum Info	Displays information about spectrum groups
Show Cable Tech Info	Displays Cable Tech information
Show HCCP details Info	Displays information on groups associated with cable interfaces
Show IGMP Info	Displays information about multicast channels and interface
Show Inline Power Info	Displays status of inline power
Show Interface Info	Displays the current configuration and status
Show Interfaces Rate-Limit Info	Displays information about committed access rate
Show IP Routing Info	Displays the current state of the routing table
Show Protocol Info	Displays protocols configured for the entire system
Show SNMP Users and Groups Info	Displays SNMP information for a specific user and group
Show Switch VLAN Info	Displays information about VLAN and interface
Show System Info	Displays version, flash, logging, hardware, route

Command Set	Commands
Show System Performance	Displays system interfaces, buffers, processes, memory
Show Tech Info	Displays system and configuration information

Managing Command Sets

The Command Set Administration task enables the administrator to view the details of an existing Command Set, create a new Command Set, edit an existing Command Set, and delete an existing Command Set.

Note You must have Administrator privileges to perform any of these tasks.

- Viewing Command Set Details
- Creating a New Command Set
- Editing Command Sets
- Deleting Command Sets
- Adding and Deleting Adhoc Commands
- System-Defined Command Sets

Viewing Command Set Details

You can view the details of an existing Command Set using this feature.

To view the Command Set details:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Command Sets**.

The Command Sets window appears.

Step 2 Click the name of a Command Set in the List of Command Sets.

The Command Set Details pop-up window appears.

Step 3 Expand each of the list tree to view details of the Command Set assigned to each of the device category in the list.

Step 4 Click **Close** to close the Command Set Details window.

Creating a New Command Set

You can create a new Command Set using this feature.

To create a new Command Set:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Command Sets**.

The Command Sets window appears.

Step 2 Click **Create** in the Command Sets window.

The Select Device Category window appears.

Step 3 Enter the name of the Command Set in the Name field and a description for the Command Set in the Description field.

Step 4 Select the type of device from the Device Type Selector.

Step 5 Click **Next** to continue.

The Select Commands window appears.

Step 6 Select the command or commands you want to assign to the selected device or group of devices from the Available Commands pane in the Select Commands window.

- Select **All Commands** from the Commands Selection drop-down list to list all the commands available for the device or group of devices.
- Select **Common Commands** from the Commands Selection drop-down list to list only the common commands.

If you have a device category with no commands, it will not be considered for populating the **Common Commands** list.

Step 7 Click **Add** to add the selected commands.

The commands move to the Selected Commands pane in the Select Commands dialog box.

Step 8 Select commands from the Selected Commands pane and click **Remove** button to delete command(s) from the Selected Commands pane.

If you want to enter adhoc commands:

a. Enter them in the Adhoc Commands text box and click **Add Adhoc**.

The adhoc commands) are added in the Available Commands pane.

b. Select thecommands that you want to assign from the Available Commands and click **Add**.

See Adding and Deleting Adhoc Commands for more details on Adhoc Commands.

Step 9 Click **Finish** to create the new Command Set.

A message appears: `Command Set` *Command Set name* `created successfully`.

Step 10 Click **OK**.

The new Command Set appears in the List of Command Sets in the Command Sets Page.

Editing Command Sets

You can edit Command Sets using this feature. You can edit only user-defined Command Sets.

To edit a Command Set:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Command Sets**.

The Command Sets window appears with the List of Command Sets.

Step 2 Select the name of the Command set in the List of Command Sets and click **Edit**.

The Select Device Category window appears with the device types that you have already selected and the Command Set name.

If you want to edit the Command Set for the particular device type, select the device type and click **Next**.

The Select Commands window appears.

Step 3 Select the command or commands you want to assign to the selected device or group of devices from the Available Commands pane in the Select Commands window.

- Select **All Commands** from the Commands Selection drop-down list to list all the commands available for the device or group of devices.
- Select **Common Commands** from the Commands Selection drop-down list to list only the common commands.

If you have a device category with no commands, it will not be considered for populating the **Common Commands** list.

Step 4 Click:

- **Add** to add the selected commands.

  Thecommands move to the Selected Commands pane in the Select Commands dialog box.
- **Remove** to delete commandsfrom the Selected Commands pane.
- Enter the commands in the Adhoc Commands text box and click **Add Adhoc**.
- Select the adhoc commands from the Selected Commands pane and click **Delete Adhoc** to remove the adhoc commands.

See Adding and Deleting Adhoc Commands for more details on Adhoc Commands.

Step 5 Click **Finish** to edit the Command Set.

A message appears: `Command Set` *Command Set name* `edited successfully`.

Step 6 Click **OK**.

Deleting Command Sets

You can delete a Command Set or a list of Command Sets using this option. You can delete only user-defined Command Sets.

To delete Command Sets:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Command Sets**.

The Command Sets window appears.

Step 2 Select the Command Sets you want to delete in the List of Command Sets and click **Delete**.

A message appears: `Selected Command Set(s) will be deleted`.

Step 3 Either:

- Click **OK** to confirm the deletion of the Command Sets.

Or

- Click **Cancel** to cancel the deletion of the Command Sets.

Adding and Deleting Adhoc Commands

You can enter the following adhoc commands while creating a command set:

`show`, **`version`**, **`where`**, **`ping`**, **`traceroute`**, and **`?`**

You can use the short forms of these commands. For example you can use **`sh`** for **`show`**.

To add and delete Adhoc Commands:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Command Sets**.

The Command Sets window appears.

Step 2 Click **Create** in the Command Sets window.

The Select Device Category window appears.

Step 3 Enter the name of the Command Set in the Name field and a description for the Command Set in the Description field.

Step 4 Select the type of device from the Device Type Selector.

Step 5 Click **Next** to continue.

The Select Commands window appears.

Step 6 Enter the adhoc commands in the Adhoc Commands text box and click **Add Adhoc**.

You can enter multiple commands; separate them by commas.

The adhoc commands are added to the Available Commands list.

- Select the adhoc commands from the Available Commands list and click **Add**.

  The adhoc commands are added to the Selected Commands list.

- Select the adhoc command(s) from the Selected Commands list and click **Remove** to remove them from the Command Set.

You can delete the adhoc commands permanently only if they are not assigned to any Command Set.

Step 7 Click **Finish** to create the new command set.

A message appears: `Command Set` *Command Set name* `created successfully`.

Step 8 Click **OK**.

The new Command Set appears in the List of Command Sets in the Command Sets Page.

Assigning Command Sets

Network Administrators can assign command sets to NetWork Operators to authorize them with executable Command Sets.

By default, all system-defined command sets are assigned to Network Administrators and Network Operators.

The Assigning Command Sets feature in NetShow allows you to specify which user or set of users can run NetShow commands.

Your login determines whether you can use this option.You can use the Assigning Command Sets feature in Netshow for:

- Showing Assigned Command Sets
- Assigning Command Sets to Users
- Assigning Custom Command Execution Privilege

Showing Assigned Command Sets

You can view the list of user-defined Command Sets assigned to a particular user using this feature.

To show the assigned Command Sets:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Assigning Command Sets**.

The Assigning Command Sets page appears with the Assign Command Sets window.

Step 2 Enter the username in the Username field and click **Show Assigned**.

The username must be that of a valid CiscoWorks user. If RME has been registered with a Cisco Secure ACS Server, then the username must be that of a valid ACS user.

The Command Sets assigned to this user appears in the Selected User-Defined Command Sets pane in the Assign Command Sets window.

Assigning Command Sets to Users

To assign Command Sets to users:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Assigning Command Sets**.

The Assign Command Sets dialog box appears.

Step 2 Enter the username in the Username field.

Step 3 Select the Command Sets that you want to allocate to the user from the Available User-Defined Command Sets list and click **Add**.

The selected Command Sets appear in the Selected User-Defined Command Sets list.

Step 4 Add all the required Command Sets to the Selected User-Defined Command Sets list box.

Step 5 Click **Assign** to assign the Command Sets access privileges to the specified user.

For a specified user to see the assigned Command Sets, enter the username in the Username field and click **Show Assigned**.

The Command Sets assigned to the user appear in the Selected User-Defined Command Sets list.

Assigning Custom Command Execution Privilege

You can assign custom command execution privilege to selected users, using the Assigning Command Set feature. You can assign this privilege to one or more users. These users can enter custom commands while creating NetShow jobs only if this privilege is enabled.

To assign Custom Command Execution privilege:

Step 1 Select **Resource Manager Essentials > Tools > NetShow > Assigning Command Sets**.

The Assign Command Sets dialog box appears.

Step 2 Enter the username in the Username field.

Step 3 Check the Custom Command Execution check box to assign custom command execution privilege to this user.

Launching show Commands From Device Center

You can run `show` commands from Device Center.

To run `show` commands from Device Center:

Step 1 Select **Device Troubleshooting > Device Center**.

The Device Center window appears with the device selector on the right and Device Center overview information on the left section of the screen.

Step 2 Either:

- Enter the device name of the device you want to select and click **Go** in the Device Selector field.

Or

- Select a device from the list-tree.

The Device Summary and Functions Available panes appear in the right section of the screen.

Step 3 Select **Run Show Command** from the Management Tasks tab under the Functions Available pane.

The Select Command Set window appears.

Step 4 Select the Command Set from the Command Set List pane in the Show Commands Execution window.

Step 5 Enter the custom commands in the Custom Commands text box.

Step 6 Click **Next**.

The Set Schedule Options page appears with the Job Schedule and Options dialog box.

Step 7 Enter the following information:

Field	Description
Scheduling	
Run Type	The Run Type of the job. The Run Types could be any or all of these, depending on the type of the job: • Immediate—Runs the job immediately. • Once—Runs the job once at the specified date and time. • 6 - hourly—Runs the job every 6 hours, starting from the specified time. • 12 - hourly—Runs the job every 12 hours, starting from the specified time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. • Last day of Month—Runs on the last day of the month at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3. To change, select the required run type from the drop-down list.
Date	Scheduled date and time of the job.
Job Information	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter your comments for the job. Comments appear in the Job Work Order.
Job Options	
Enable Job Password	• If you have enabled the Enable Job Password option and disabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) enter the device login user name and password and Device Enable password. • If you have enabled the Enable Job Password option and enabled the User Configurable option in the Job Policy dialog box (Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies) either: – Enter the device login user name and password and Device Enable password. Or – Disable the Job Password option in the Job Schedule and Options dialog box.

Field	Description
Execution	Specify the order in which the job should run on the devices. • Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. • Sequential—Allows the job to run on only one device at a time.
Maker Comments	This field appears only if you have enabled Job Approval Policies for NetShow. Enter the Maker Comments. See Setting Up Job Approval for more details on enabling Job Approval Policies.
Maker E-mail	This field appears only if you have enabled Job Approval Policies for NetShow. Enter the Maker E-mail address. This is mandatory. See Setting Up Job Approval for more details on enabling Job Approval Policies.

Step 8 Click **Next**.

The View Job Work Order page appears with the Job Work Order.

The Job Work Order contains general information on the job and on the:

- Job policies.
- Job approval details (if you have enabled job approval).
- Device details.
- Command Sets and the commands to be run.

Step 9 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A message appears, `Job ID created successfully`.

The newly created job appears in the NetShow Job Browser.

Using cwcli netshow Command

You can invoke Netshow features from Command Line Interface (CLI).

The **`cwcli netshow`** command let you use NetShow features from the command line. You can use the **`cwcli netshow`** commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

This command is described in the cwcli framework chapter. For details see the topic Running cwcli netshow Command in the section Overview: cwcli netshow Command.

Administering NetShow Settings

NetShow supports the following Administration options in RME:

- Configuring Job Policies
- Setting Log Levels
- Assigning Approval Lists
- Setting Up Job Approval
- Generating a Standard Audit Trail Report

Configuring Job Policies

Each NetShow job has properties that define how the job runs. You can configure a default policy for these properties that apply to all future jobs. For each job property you can specify whether users can change the default property when creating a job.

NetShow supports the following Job Policies:

- Defining Default Job Policies

  The default job policies that NetShow support are E-Mail Notification, Enable Job Password, and Execution Policy.
- Purging Jobs

  The Job Purge option provides a centralized location for you to schedule purge operations.
- Defining Protocol Order

  You can define the protocol order for NetShow through the Protocol Ordering option in the Config Management feature in RME.

Defining Default Job Policies

NetShow supports E-Mail Notification, Enable Job Password, and Execution Policy.

Note View Permission Report (**Common Services > Server > Reports)** to check if you have the required privileges to perform this task.

To define these default Job Policies:

Step 1 Select **Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**.

The Job Policy dialog box appears.

Step 2 Select **NetShow** from the Application drop-down list.

Step 3 Enter the following information in the Job Policy dialog box:

Field Name	Description	Usage Notes
E-mail Notification	Enter the e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses; separate these addresses by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.	Notification is sent when job is started and completed. Notification e-mails include a URL to enter to display job details. If you are not logged in, log in using the login panel.
Enable Job Password	The Job Password Policy is enabled for all the jobs. NetShow jobs use this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository. These device credentials are entered while scheduling a job.	You can use this option even if you have configured only the Telnet password (without configuring username) on your device. You must enter a string in the Login Username field. Do not leave it blank. The Login Username string is ignored while connecting to the device since the device is configured only for the Telnet password.
Execution Policy	Allows you to configure the job to run on multiple devices at the same time (Parallel Execution) or in sequence (Sequential Execution).	None.

Step 4 Click **Apply**.

A message appears, `Policy values changed successfully`.

Step 5 Click **OK**.

Purging Jobs

The Job Purge option provides a centralized location for you to schedule purge operations for certain RME jobs including NetShow jobs.

Select **Resource Manager Essentials > Administration > System Preferences > Job Purge** to invoke the Job Purge option.

The Job Purge window contains the following information:

Column	Description
Application	Lists the application for which the purge is applicable.
Status	Whether a purge job is enabled or disabled.
Policy	This value is in days. Data older than the specified value, will be purged. You can change this value as required. This is a mandatory field. The default is 180 days.
Job ID	Unique ID assigned to the job by the system, when the purge job was created. This Job ID does not change even if you disable or enable or change the schedule of the purge job. For the Purge Now task, a Job ID is not assigned. Also, if a Job ID already exists for that application, this Job ID is not updated for the Purge Now tasks. That is, the job scheduled for purging is not affected by the Purge Now task.
Scheduled At	Date and time that the job was scheduled at. For example: Nov 17 2004 13:25:00.
Schedule Type	Specifies the type of schedule for the purge job: • Daily—Daily at the specified time. • Weekly—Weekly on the day of the week and at the specified time. • Monthly— Monthly on the day of the month and at the specified time. (A month comprises 30 days).

To purge NetShow Jobs:

Step 1 Select **Resource Manager Essentials> Administration> System Preferences> Job Purge**.

The Job Purge dialog box appears.

Step 2 Select NetShow jobs from the list of jobs in the Job Purge dialog box.

You can perform the following tasks in the Job Purge window:

Button	Description
Schedule	Schedule a job purging.
Enable	Enable a job for purging after you schedule it.
Disable	Disable the purge after enabling a job for purging.
Purge Now	Purge a job immediately.

Defining Protocol Order

You can define the protocol order for NetShow through the Protocol Ordering option in the Config Management feature in RME.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To define the protocol order for NetShow:

Step 1 Select **Resource Manager Essentials > Admin > Config Mgmt**.

The Transport Settings dialog box appears.

Step 2 Select **NetShow** from the Application Name drop-down list.

Step 3 Select a protocol from the Available Protocols pane and click **Add**.

NetShow supports only Telnet and SSH.

If you want to remove a protocol or change the protocol order, you can remove the protocol using the **Remove** button and add the protocol, again.

The protocols that you have selected appear in the Selected Protocol Order pane.

Step 4 Click **Apply**.

A message appears, `New settings saved successfully`.

Step 5 Click **OK**.

Note The protocol used for communicating with the device is based on the order in which the protocols are listed here.

Setting Log Levels

You can use this option to set the log levels for NetShow.

Log files are stored at these locations:

- On Windows: *NMSROOT*\log, where *NMSROOT* is the CiscoWorks installation directory.
- On Solaris: /var/adm/CSCOpx/log

Locate the following log files for NetShow:

- NetShowServer.log

  All information related to the process NetShowMgr will be logged in this file.
- NetShow_cli.log

  All information related to the NetShow CLI commands will be logged in this file.
- NetShowClient.log

  All other information related to NetShow will be logged in this file.

To set the log levels for NetShow:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**.

The Set Application Logging Levels dialog box appears.

Step 2 Select **NetShow** from the Application drop-down list.

Step 3 Select the appropriate log level from the Logging Level drop-down list.

Step 4 Either:

- Click **Reset** to apply the default logging levels.

Or

- Click **Apply** to set the Log Level you have selected.

A message appears, `Successfully updated the Log levels.`

Step 5 Click **OK**.

Assigning Approval Lists

You can assign an Approver list to NetShow, from the available Approver lists.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To assign an Approver list:

Step 1 Select **Resource Manager Essentials > Admin > Approval > Assign Approver Lists**.

The Assign Approver Lists dialog box appears.

Step 2 Select the required Approver list from the drop-down list box for NetShow.

Step 3 Click **Assign**.

The selected Approver lists are assigned to NetShow.

Setting Up Job Approval

The Approval Policies dialog box allows you to set up Job Approval for NetShow.

Make sure the approver list is assigned to NetShow, before you enable approval for the application.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To set up Job Approval:

Step 1 Select **Resource Manager Essentials > Admin > Approval >Approval Policies**.

The Approval Policies dialog box appears.

Step 2 Set up Job Approval for NetShow. To do this, either:

- Select the **Enable** check box that corresponds to NetShow, to enable Job Approval.

Or

- Deselect the **Enable** check box that corresponds to NetShow, to disable Job Approval.

Step 3 Click **Apply** to apply your changes.

After you enable Job Approval, two additional fields appear in the Job Schedule wizard of NetShow. These are:

- Maker Comments—Job creator's comments.
- Maker E-mail—Job creator's e-mail address.

Generating a Standard Audit Trail Report

This option lets you compile a report on all Audit Trail changes that occurred in the network during a specific time period.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

For more information on generating the Standard Audit Trail Report, see Generating a Standard Audit Trail Report section in the Tracking RME Server Changes Using Audit Trail chapter.

The Audit Trail report contains all change information provided by RME applications based on your filter criteria. For more information on understanding the Audit Trail Report, see Understanding the Audit Trail Report section in the Tracking RME Server Changes Using Audit Trail chapter.

CHAPTER 12

Managing Software Images Using Software Management

Manually upgrading your devices to the latest software version can be an error-prone, and time-consuming process. To ensure rapid, reliable software upgrades, Software Management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring.

Using Software Management, you can:

- Set up your Software Management preferences.

  You can specify information such as, the directory where images are stored, the pathname of the user-supplied script to run before and after each device software upgrade, etc.

  You can enable and define the protocol order for Software Management tasks. You can also enable the Job Based Password option for Software Management tasks.

  You can specify if the images on Cisco.com should be included during image recommendation of the device. Also specify the Cisco.com filters so that only the images that match the filter criteria are selected.

  See Viewing/Editing Preferences for further details.

- Analyze software upgrades

  You can generate Upgrade Analysis reports that help you determine prerequisites for a new software deployment.

  These reports analyze the proposed images to determine the hardware upgrades (device access, boot ROM, Flash memory, RAM, and NVRAM and boot Flash, if applicable) required before you can perform the upgrade.

  See Upgrade Analysis for further details.

- Import images into the software repository

  You can determine the images missing from your repository and import them into the software repository.

  You can also keep the repository up-to-date and periodically synchronize the repository with the images running on your network devices.

  You can also schedule an image import for a later, more convenient time.

  See Adding Images to the Software Repository for further details.

- Distribute software images to groups of devices

  Depending on system complexity, you can configure upgrades for groups of devices to the same software image or to different software images.

You can specify these groups manually, using your RME groups and search criteria. You can also use some other selection criterion, such as the current software version or hardware type.

You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

See Software Distribution for further details.

- Distribute images as patches to group of devices

  Depending on system complexity, you can configure upgrades for groups of devices to the patch software images.

  You can specify these groups manually, using your RME groups and search criteria. You can also use some selection criterion, such as the current software version or hardware type.

  You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

  See Patch Distribution for further details.

- Reduce errors by using a recommended image

  Software Management checks the current software version, Flash device size, DRAM size, boot ROM version. Software Management also checks any device type specific software and hardware requirements for compatibility. Software Management checks and recommends a best-fit image for a device.

  See Understanding Upgrade Recommendations for further details.

- Schedule image upgrade jobs

  You can schedule image upgrades to occur immediately or at a later, more convenient time. Optionally, you can integrate software upgrade scheduling into your internal change approval process (**Resource Manager Essentials > Admin > Approval**).

  After an upgrade, you can:

  - Undo the upgrade and roll back to the previous image

    Software Management tracks each device's image history so that if you upgrade to a new image, you have a record of what has been installed on the device. This allows you to undo the upgrade and roll back to the previous image, if necessary.

    An Change Audit record is logged for this task. You can generate the Standard Change Audit report using **Resource Manager Essentials > Reports > Report Generator**.

    See Undo a Successful Distribution Job for further details.

  - Retry the upgrade on devices that failed in a previous job

    You can also retry a job for devices that failed the upgrade process. For example, you may need to do this because of a configuration error or a bad network connection.

    You can retry the job and include only those devices that were not upgraded previously.

    See Retry a Failed Distribution Job for further details.

- Track job progress and job history information

  Software Management generates detailed job reports. These reports display the status of each software upgrade and a detailed job log. They also keep track of job and device operations and job history information.

  See Using Software Management Job Browser for further details.

- Track software bugs

You can view the known catastrophic or severe bugs in the software running on the devices supported by Software Management using Bug Toolkit (**Resource Manager Essentials > Reports > Report Generator**).

See Checking Bug Status Using Bug Toolkit for further details.

- Set the debug mode for Software Management application

  You can set the debug mode for Software Management application in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

  See Application Log Level Settings for further details.

- Using Device Center you can perform the following Software Management tasks:
  - Add Images to Software Repository (from Devices)
  - Determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com using Cisco.com Image
  - Determine the impact to and prerequisites for a new software deployment using images that reside in Software Repository
  - Distribute Images (by Devices, Basic)

  See RME Device Center for further details.

- The supported IOS image version for RME 4.1 is 11.x and later.

For the new features in this release, see What's New in this Release.

For list of supported devices in the Software Management application, see:

- Supported Image Import Features for Software Management

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baab.html

- Supported Image Distribution Features for Software Management

  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baaa.html

Setting Up Your Environment

This section lists all prerequisites for using the Software Management application:

- Requirements on CiscoWorks Server
- Logging Into Cisco.com
- Configuring Devices for Upgrades
- Using Job Approval for Software Management

Requirements on CiscoWorks Server

The following are the prerequisites:

- Make sure you have a directory or file system location with enough space to store the software images.

- Verify that you have the appropriate privilege level to access Software Management options. You can view the Permission Report (**Common Services > Server > Reports > Permission Report**) to know the various RME privilege levels.
- If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site.
- If your system is behind a firewall, configure the proxy URL to access the Internet from the installed system. You can do this using **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**

  You can enter Cisco.com credentials when you use the Software Management tasks.

  See Logging Into Cisco.com for further details.

Mandatory Setup Tasks

- Add the device passwords to the Device and Credentials database. You can add these credentials using **Common Services > Device and Credentials > Device Management**. Also, see Configuring Telnet and SSH Access for further details.
- Use the **Common Services > Server > Admin > System Preferences** option to enter the name of your SMTP server. You have to configure the SMTP server to send e-mails.

  We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
- If you plan to enable a remote file copy (rcp) or secure copy server as the active file transfer server, see Configuring rcp or Configuring SCP for further details.
- Set or change your Software Management preferences. See Software Management Administration Tasks for further details.

Optional Setup Tasks

- Make a baseline of your network images by importing images from the Software Management-supported devices in your network into your software image repository.

  To do this, go to **Resource Manager Essentials > Software Mgmt > Software Repository** and click **Add** and select **Device**.
- Schedule the Synchronization report to run periodically. This is used to determine whether any images running on Software Management-supported devices are not in the software image repository.

  To do this, go to **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.
- If you use the Job Approval option to approve or reject jobs, you must create one or more approver lists and enable Job Approval. To enable Job Approval use **Resource Manager Essentials** > **Admin > Approval**.

Logging Into Cisco.com

Login privileges are required for all Software Management tasks that access Cisco.com.

If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site.

To download the cryptographic images on Cisco.com through Software Management tasks, you must have a Cisco.com account with cryptographic access.

To get the access you must have a Cisco.com account. You can register by going to the following URL:

http://tools.cisco.com/RPF/register/register.do

After getting the Cisco.com account:

Step 1 Go to the following URL: http://www.cisco.com/pcgi-bin/Software/Crypto/crypto_main.pl

The Enter Network Password dialog box appears.

Step 2 Log in with your Cisco.com account.

The Encryption Software Export Distribution Authorization Form page appears.

Step 3 Select your software from the list box and click **Submit**.

The Encryption Software Export Distribution Authorization Form appears.

Step 4 Review and complete the Encryption Software Export Distribution Authorization form and click **Submit**.

The `Cisco Encryption Software: Crypto Access Granted` message appears.

Note It takes approximately 4 hours to process your application. You cannot download the software until the entitlement process is complete. You will not receive any notification for this.

On CiscoWorks server, you can enter Cisco.com credentials in two ways:

- Common Cisco.com credentials for all users of CiscoWorks server.
- Individual user Cisco.com credentials

To configure common Cisco.com credentials for all users of CiscoWorks server:

Step 1 Select **Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup**.

The Cisco.com User Account Setup dialog box appears.

Step 2 Enter the following:

- Username—Login ID of the Cisco.com User.
- Password—Password of the Cisco.com User.
- Verify Password—Password to confirm.

Step 3 Click **Apply** to save the user details.

You can enter your individual Cisco.com credentials when you perform any Software Management tasks that need access to the Cisco.com server.

If your Cisco.com username and password have not been added to the CiscoWorks database, enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, the credentials are valid only for that session.

If you Cisco.com username and password have been added to the CiscoWorks database, then Cisco.com login dialog box appears with the information that is available in the CiscoWorks database.

If you are accessing Cisco.com over a proxy server, you must enter the proxy server details in the Proxy Server Setup dialog box (**Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**).

Using Job Approval for Software Management

You can enable Job Approval for Software Management tasks, (**Resource Manager Essentials > Admin > Approval > Approval Policies**) which means all jobs require approval before they can run.

Only users with Approver permissions can approve Software Management jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

The following Software Management tasks require approval if you have enabled Job Approval:

- Adding images to Software Repository (**Resource Manager Essentials > Software Mgmt > Software Repository > Add**) using:
  - Cisco.com
  - Device
  - URL
  - Network
- Distribution software images (**Resource Manager Essentials > Software Mgmt > Software Distribution**) using any one of these methods:
  - Distributing by Devices [Basic]
  - Distributing by Devices [Advanced]
  - Distributing by Images
  - Remote Staging and Distribution

If you have enabled Approval for Software Management tasks, then in the Job Schedule and Options dialog box, you get these two options:

- Maker Comments—Approval comments for the job approver.
- Maker E-Mail—E-mail ID of the job creator.

See Enabling Approval and Approving Jobs Using Job Approval for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Software Management Administration Tasks

You can set your preference to download images and upgrade your knowledge base. To do this, go to **Admin > Software Mgmt**.

The following sections explain how to set the Software Management preferences and upgrade your knowledge base:

- Viewing/Editing Preferences
- Updating Upgrade Information

Viewing/Editing Preferences

Edit Preferences helps you to set or change your Software Management preferences.

The options you specify here are applicable to Software Management tasks such as image distribution, image import, etc.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To view and edit the preferences:

Step 1 Select **Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences**.

The View/Edit Preferences dialog box appears.

Step 2 Enter the following:

Field	Description	Usage Notes
Repository Management		
Image Location	New directory to store software images. By default the software images are stored at this location: On Solaris: /var/adm/CSCOpx/files/rme/repository/ On Windows: *NMSROOT*/files/rme/repository Where *NMSROOT* is the CiscoWorks installed directory.	If you enter a new name, *all existing files* are moved to this directory. If the directory does not have enough space, the files are not moved and an error message appears. If the specified directory does not exist, Software Management creates a new directory before moving the files to the new directory. The new directory should be empty. The new directory specified by you should have the permission for *casuser*:*casusers* in Solaris and *casuser* should have Full Control in Windows.

Field	Description	Usage Notes
Distribution		
Script Location	You can specify only shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows. The script files *must* be available at this location: On UNIX: /var/adm/CSCOpx/files/scripts/swim On Windows: *NMSROOT*/files/scripts/swim To select the script file: **a.** Click **Browse**. The Server Side File Browser dialog box appears with the predefined location. **b.** Select the script file (*.sh on Unix and *.bat on Windows) **c.** Click **OK**. You can use **Clear** to clear your selections for Script Location. This clears all previous values.	On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission. On Windows, the script should have read, write, and execute permissions for casuser/Administrator. The other users should have only read permission. You must ensure that the scripts contained in the file have permissions to execute from within the *casuser* account. This script is run before and after completing each device software upgrade for all scheduled jobs. See Understanding User-supplied Scripts for further information on variable parameters that you can provide in a script.
Script Timeout (seconds)	Number of seconds the user's script can run (default = 90).	Software Management waits for the time specified before concluding that the script has failed.
Protocol Order	Specify an order of preferred protocol for image import/distribution. The supported protocols are: • RCP • TFTP • SCP • HTTP See Selecting and Ordering Protocol Order for further details. Also, see Configuring Devices for Upgrades.	This preferred protocol order is followed only for those devices that permit more than one protocol for image transfer. In devices, where multiple protocol option is not available for image transfers, Software Management uses its own knowledge and selects the relevant protocol to upgrade the device. For fetching configuration from device, the protocol settings of Configuration Management is used. Software Management uses the same protocol for fetch and download of configurations. You can set the Configuration Management protocol order using Resource Manager Essentials > Admin > Config Mgmt.

Field	Description	Usage Notes
Use SSH for software image upgrade and software image import through CLI.	Uses this protocol to connect to the devices. By default, Telnet is used to connect to the devices. If the SSH fails, there is no fallback.	The device must support SSH for Software Management to use this protocol. Software Management uses command line interface to upgrade software images and to import software images. When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2. If so, it tries to connect to the device using SSHv2. If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1. If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2. If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed. See the Software Management Functional Supported Device tables on Cisco.com for SSH and CLI device support information. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html
Recommendation Filters (See How Recommendation Filters Work for an IOS Image.)		
Include Cisco.com images for image recommendation	During image distribution, recommend Cisco.com images for Cisco devices.	
Include General deployment images	Includes only GD images.	For Cisco IOS devices only.
Include latest maintenance release (of each major release).	Includes the latest major releases of IOS images. For example, if Release 12.2(5) was latest maintenance version in the 12.2 major release, the recommended image is IOS 12.2(5).	For Cisco IOS devices only.
Include images higher than running image.	Includes the images that are newer than the images running on your device. For example, if the device is running Release 11.2(3), the recommended images are 11.2(4) and later.	For Cisco IOS devices only.

Field	Description	Usage Notes
Include same image feature subset as running image.	Include only images that have the same feature subset as the current image. For example, if you want IOS images with the ENTERPRISE IPSEC feature, the recommended images contain the latest version. This version contains feature subset that fits the Flash.	For Cisco IOS devices only.
Password Policy		
Enable Job Based Password	Enter a username and password for running a specific Software Management job. If you enter a username and password, Software Management application uses this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository.	• If you have enabled User Configurable option, you can disable this option while scheduling the distribution jobs. • If you have disabled User Configurable option, you must enter the username and password while scheduling the distribution jobs. These passwords are used only to connect to devices for which Software Management uses CLI, Telnet, and SSH.for software upgrades. See the Software Management Functional Supported Device tables on Cisco.com for CLI, Telnet and SSH device support information. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Step 3 Either:

- Click **Apply** to save your changes.
- Click **Defaults** to display the default configuration.
- Click **Cancel** to discard the values entered and revert to previously saved values.

Selecting and Ordering Protocol Order

In the View/Edit Preferences dialog box (**Admin > Software Mgmt > View/Edit Preferences**) you can define the protocol order that Software Management has to use for software image download.

Software Management tries to download the software images based on the specified protocol order.

While downloading the images, Software Management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until Software Management finds a transport protocol for downloading the images.

To Enable the Protocols:

Step 1 Select a protocol from the Available Protocols pane.

Step 2 Click **Add** or double click the mouse.

To Disable the Protocols:

Step 1 Select a protocol from the Selected Protocol Order pane.

Step 2 Click **Remove** or double click the mouse.

To Reorder the Protocols

Step 1 Select the protocols from the Selected Protocol Order pane.

Step 2 Click **Remove**.

You can either select the protocols individually or use the mouse to select all of them and click **Remove**.

Step 3 Select a protocol from the Available Protocols pane.

Step 4 Click **Add** or double click the mouse.

How Recommendation Filters Work for an IOS Image

This section describes how the recommendation filters that you select in the View/Edit Preferences dialog box (**Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences**) work for a Cisco IOS image.

If you have selected the option, Include Cisco.com Images for image recommendation, Software Management checks for the images that are available on Cisco.com and the Software repository.

If the same image is available in the Software repository and Cisco.com, the image is recommended from the Software repository.

If you have not selected the option, Include Cisco.com Images for image recommendation, the Software Management checks and recommends images only from Software repository. SeeTable 12-1 for details

Table 12-1 Recommending Images for an Cisco IOS Image

Option Number	Include General Deploy-ment Images	Include Latest Maintenance Release (of Each Major Release)	Include Images Higher Than Running Image	Include Same Image Feature Subset as Running Image	Recommendation
1	Not selected	Not selected	Not selected	Not selected	The recommendation image list includes: • All available images. • In case of, – Multiple images with the same version as that of the running image version are present, the image with a higher compatible feature than the running image is recommended. – Similar images in Cisco.com and Software Management repository, the image from the repository is recommended. • The image feature can be the same or a superset of the running image. If a higher version is not available, then no recommendation is made.
2	Not selected	Not selected	Not selected	Selected	The recommended list contains images that have the same feature set as that of the running image. The images with the highest version among the recommended image list are recommended.
3	Not selected	Not selected	Selected	Not selected	The recommend list contains all types of releases (deployment status). The images with the highest version among recommended image list are recommended. The feature set of the recommended image may be superior than the running image.
4	Not selected	Selected	Not selected	Not selected	The latest maintenance version in each release is available in the recommend image list. The latest image version is recommended.
5	Selected	Not selected	Not selected	Not selected	The images with deployment status identified as GD are available in the recommended image list and other recommendation flow remains the same as the option 1.
6	Selected	Not selected	Not selected	Selected	Same as option5. However, the recommended list contains images that have the same feature set as that of running image.
7	Selected	Not selected	Selected	Not selected	Same as option 5. However, the image with the highest version in the recommended image list is recommended. The feature set of the recommended image may be superior than the running image.
8	Selected	Not selected	Selected	Selected	Same as option 6. However, the image with the highest version in the recommended image list is recommended. All recommend images will have the same feature subset as the running image.

Table 12-1 Recommending Images for an Cisco IOS Image (continued)

Option Number	Include General Deployment Images	Include Latest Maintenance Release (of Each Major Release)	Include Images Higher Than Running Image	Include Same Image Feature Subset as Running Image	Recommendation
9	Selected	Selected	Not selected	Not selected	The images with the highest version among recommended image list are recommended. The images of GD types of releases are available in the recommended image list.
10	Selected	Selected	Not selected	Selected	The images with the same feature as that of running image is available in the recommended list and the latest maintenance version of all release is available in the recommended list. Only an image with higher version than running image is recommended. The recommended images can have only GD status.
11	Selected	Selected	Selected	Not selected	Same as option 9. In addition to this, an image with the higher version than running image is also recommended.

Updating Upgrade Information

For IPX/IGX/BPX/MGX devices, both the Cisco.com Upgrade Analysis and the Repository Upgrade Analysis options use the upgrade knowledge base to make upgrade recommendations.

See Upgrade Analysis for further details on how to Upgrade Analysis from Cisco.com and Repository.

The following table identifies the knowledge bases and the Upgrade Analysis Report recommendations generated from each:

Upgrade Knowledge Base	Upgrade Analysis Report
IPX/IGX/BPX/MGX Memory and Upgrade Path	RAM Upgrade BRAM Upgrade Upgrade Path
IPX/IGX/BPX/MGX Firmware Compatibility	Module Firmware Upgrade Firmware Compatibility

The information source for IPX/IGX/BPX/MGX is the software release notes for these devices.

Note You should always review the Release Notes before performing any upgrade because important information that supplements the Upgrade Analysis Report may be provided.

Since the knowledge bases change periodically as new images are released, the knowledge base files are maintained on Cisco.com. The Update Upgrade Information option allows you to update your RME server to the latest versions of these files.

An administrator should update the knowledge bases regularly if IPX/IGX/BPX/MGX device upgrades are performed. If your RME server is connected to Cisco.com, you can update the knowledge bases directly from Cisco.com.

Otherwise, you must retrieve the files from Cisco.com using some other system, move the files to a local directory on your server, and then import them.

Before You Begin

Ensure that you download the latest knowledge base files from Cisco.com to your local filesystem. This is important if your RME server is not connected to Cisco.com

The files are located at ftp.cisco.com: /cisco/netmgmt/cw2000/essentials/swim-kb/

Review the Readme file in that directory to determine the latest knowledge base files.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To update the knowledge base:

Step 1 Select **Resource Manager Essentials > Admin > Software Mgmt > Update Upgrade Information**.

The Upgrade Knowledge Base dialog box appears.

Step 2 Click **Update**.

The Update Upgrade Information Source dialog box appears.

Step 3 Either:

a. Click **Cisco.com** if you have connection from your RME server to Cisco.com.

   If your Cisco.com username and password have not been added to the CiscoWorks database, a dialog box appears.

b. Enter your Cisco.com username and password.

   The credentials you enter here are valid only for that session.

If your Cisco.com username and password have been added to the CiscoWorks database, the Cisco.com login dialog box appears with the information that is available in the CiscoWorks database.

Or

a. Click **File System** if you do not have a connection from your RME server to Cisco.com and if you have downloaded the knowledge base files from Cisco.com to the RME server.

b. Enter the path to one of the files.

Step 4 Click **Next**.

The Update Upgrade Information Verification window appears with the following information:

Field	Description
File	Name of the device and the supported upgrade knowledge base information.
Available Version	Version of this knowledge base currently installed in the RME system.
Current Version	Available version of this knowledge base in the Cisco.com or the File System of the server.
Comparison Result	Results of the verification of the knowledge base to check if it is up to date or needs an upgrade.

Step 5 Click **Finish**.

Software Repository

The Software Repository Management window displays the images that are available in the Software Management repository. This window contains the following fields, buttons, and the entry in the TOC:

- Software Repository Management Fields (Table 12-2)
- Software RepositoryManagement Window Buttons and TOC Entry Table 12-3

Table 12-2 Software Repository Management Window Fields

Fields	Description
File Name	File name of the software image. Click on the File Name to edit the image attributes. See Editing and Viewing the Image Attributes.
Image Family	Name of the image family.
Image Type	Type of the images (SYSTEM_SW, SUPERVISOR, SUPERVISOR2_6000, SUPERVISOR6000, BOOT_LOADER, ATM_WBPVC, etc.).
Version	Software version number.
Size	Image size in megabytes.
Status	Status of the image on Cisco.com. See Synchronizing Software Image Status With Cisco.com.
Updated at	Date and time the image was checked into the repository.
Comments	Comments, typically used to track why the image was added to repository.

Table 12-3 Software Repository Management Window Buttons and TOC Entry

Buttons and TOC Entry	Description
Software Repository Synchronization (TOC entry)	Keep the software repository up to date. See: • Software Repository Synchronization • Scheduling a Synchronization Report • Viewing a Synchronization Report • Removing a Synchronization Report Job
Filter (Button)	Filter and search images. See Searching for Images From the Software Repository.
Add (Button)	Add images to the repository. See Adding Images to the Software Repository.
Delete (Button)	Delete images from the repository. See Deleting Images From the Software Repository.
Export (Button)	Export images from Repository. See Exporting of Images from Software Repository.
Update Status (Button)	Update the status of the images. See Synchronizing Software Image Status With Cisco.com.

Software Repository Synchronization

The Synchronization report shows which Software Management-supported devices are running software images that are not in the software image repository.

Using this option you can view the Synchronization report and schedule the synchronization report.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Select **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.

The Software Repository Synchronization dialog box that appears contains the following. SeeTable 12-4:

Table 12-4 Software Repository Synchronization Dialog Box

Fields/Buttons	Description
Job Id	Unique number assigned to the job when it is created.
Next Run	Time and date of the next instance of Synchronization Report job.

Table 12-4 Software Repository Synchronization Dialog Box (continued)

Fields/Buttons	Description
View Report	You can view the synchronization report. This report displays which Software Management-supported devices are running software images that are not in the software image repository. See Viewing a Synchronization Report for further details.
Schedule	You can schedule a Synchronization report. You can also reschedule a existing Synchronization report. See Scheduling a Synchronization Report for further details.
Remove Job	You can remove the scheduled synchronization report job. See Removing a Synchronization Report Job for further details.

Scheduling a Synchronization Report

To schedule or reschedule a Synchronization report:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **Schedule**.

The Job Schedule for Out-of-sync Report dialog box appears.

Step 3 Enter the following information:

Field	Description
Scheduling	
Run Time	You can specify when you want to run the Image Out-of-Sync Report job. To do this, select one of these options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	

Field	Description
Job Description	The system default job description, *SoftwareImages Out Of Synch Repor*t is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 4 Click **Submit**.

If the job was scheduled successfully, the notification dialog box is displayed with the Job ID.

You can check the status of your scheduled synchronization job by selecting **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

Viewing a Synchronization Report

To view a synchronization report:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **View Report**.

The Image Out-of-synch Report window appears.

Removing a Synchronization Report Job

To remove a Synchronization Report job:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **Remove Job**.

A confirmation dialog box shows that the synchronization report job is removed successfully.

Step 3 Click **OK**.

Adding Images to the Software Repository

Your software image repository should contain copies of software images running on all Software Management-supported devices in your network. Use the following options to populate and maintain your software repository:

- The Add Image to Software Repository using the Cisco.com option downloads images for devices in RME from Cisco.com to the software repository.

  See Adding Images to the Software Repository From Cisco.com.
- The Add Image to Software Repository using the Device option
  - Imports images from selected Cisco devices to the software repository.
  - Imports software from Flash cards on a live device to the software repository.

  See Adding Images to the Software Repository From Devices.
- The Add Image to Software Repository using the File System option imports an image from a directory accessible from the RME server.

  See Adding Images to the Software Repository From a File System.
- The Add Image to Software Repository using the URL option downloads images from URL you specify.

  See Adding Images to the Software Repository From a URL.
- The Add Image to Software Repository using the Network option creates a baseline of all Software Management-supported devices in your network, and imports these images into your software repository.

  See Adding Images to the Software Repository From the Network.

Adding Images to the Software Repository From Cisco.com

Use this option to download software images from Cisco.com into the software image repository.

- Contact your channel partner or enter a request on the main Cisco web site. If you do not have a user account and password on Cisco.com.

  See Logging Into Cisco.com.
- Access the Cisco.com web site to make sure that the releases for the images you plan to download are stable.
- Determine the approximate number and size of the images you want to download. The number of images you can download at a time can vary depending on Cisco.com load, image sizes, network load, RME server load, and so on.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To add images from Cisco.com:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Cisco.com**.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

- Enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.
- You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

  Common Services > **Security** > **Cisco.com Connection Management Proxy Server Setup**
- After entering the credential information, Click **OK**.

Step 4 Click **Next**.

The Device Selection dialog box appears.

Step 5 Select the device from the Device Selection dialog box, and click **Next**.

If you do not want to select any devices, click **Next**.

If you select devices from this list, they identify a subset of device software images. This helps you narrow your options on subsequent screens.

The Add Images from Cisco.com dialog box appears. This dialog box has several sections from which you select combinations of device platforms, software release versions, and software subset images.

See Using RME Device Selector for information on how to use RME Device Selector.

Step 6 Select the images to download. Work from left to right and from top to bottom:

a. From the Select a Device/Platform section, select a device or device family.

If you select an individual device, the device family, Cisco IOS release, and required Flash and RAM sizes appear.

For IPX/IGX/BPX/MGX devices, the system software release appears.

A list of available software versions for that device appears in the top middle section.

b. From the Software Versions section, select a software version.

If you are unsure of the subset image you need, see the Release Notes on Cisco.com.

- For IPX/IGX/BPX platforms, both switch software and all applicable module firmware images appear.
- For MGX platforms, system releases appear.

A list of available subset images for the selected software version appear in the top right frame.

c. From the Software Subset Images section, select a subset image.

The subset image is added to the Images to be Added table in the bottom section.

For IPX/IGX/BPX/MGX devices, there are no subset images. Select the item that appears in this section to complete image selection.

Step 7 Continue adding images to the list.

The images that you have added appear in the Images to be Added table. This table contains this information:

- Devices/Platforms—Name of the device or platform.
- Version—Software version that you have selected.
- Subset—Subset image information.

Step 8 Click **Next** when the list contains all image combinations to download.

Software Management verifies that the images in the Image list run in the selected devices and displays the status in the Add Images from Cisco.com dialog box. The Add Images from Cisco.com dialog box contains:

Field	Description
Device/Platform	Lists the device details that you have selected.
Selected Version and Subset	Displays the image details.
Image Requirements	Displays the required hardware (RAM and Flash) details.
Download	Select the image you want to download. By default, the check boxes are selected for the images that have passed the verification. You can choose not to add an image by deselecting that check box.
Pass/Fail	Results of image verification. • Pass—Device has the minimum required memory and Flash memory. • Fail—Device does not have enough memory or Flash memory. Images that fail verification on one device could work on another. Therefore, you can download a failed image by selecting the Download check box.

Step 9 Select the images to add to the image repository in the Add Images from Cisco.com dialog box and click **Next**.

The Job Control Information dialog box appears.

Step 10 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Cisco.com) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 11 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name which you have selected. It also displays the file size of the image.

Step 12 Click **Finish.**

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Software Mgmt > Software Mgmt Jobs**.

.

Adding Images to the Software Repository From Devices

Use this procedure to add software images from Cisco devices to the software repository.

You can also launch this task for a specific device using the Device Center link from CiscoWorks LMS Portal home page (**Device Troubleshooting > Device Center**).

Software Management downloads images from more than one device in parallel. You must ensure that software repository has enough free space to accommodate at least 20 images.

Where *NMSROOT* is the CiscoWorks installed directory.

The image import from device option is not available for all the devices. Find the devices from which you can download images in the Supported Image Import Features for Software Management table on Cisco.com.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To add images from devices:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Device**, and click **Next**.

The Device Selection dialog box appears in the Add Images from Device window.

See Using RME Device Selector for information on how to use RME Device Selector.

Step 4 Select the devices that contain the images to add to the software repository.

Step 5 Click **Next**.

Software Management retrieves the images, analyzes them according to the selected image type, and displays a report which contains:

Field	Description
Image	Available images on your device.
Available At	Location where the image is available on your device.
Device	Name of the device as managed by RME.
Size	Image size in bytes.
Errors	Click on the link for details.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Job Control Information dialog box appears.

Step 7 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Device) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 8 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name which you have selected. It also displays the file size of the image.

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job select **Software Mgmt > Software Mgmt Jobs**.

Adding Images to the Software Repository From a File System

Use the following procedure to add software images from a file system to the software repository.

You have to know the directory name in which the image files are stored before importing the images from the File System to the software repository.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To add images from file system:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **File System**, and click **Next**.

The Add Image From Local File System dialog box appears.

Step 4 Enter the full pathname of the source file or directory.

Or

a. Click **Browse** to search for the directory name.

   The Server Side File Browser dialog box appears.

b. Select either the file or the directory on the RME server.

c. Click **OK**.

Step 5 Click **Next**.

The Image Attributes dialog box appears with this information:

- Filename—Filename as it appears in filesystem directory.

  You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.

- Image Type—Image type, determined from the filename. If the image type is not correct, select correct type from drop-down list box.

  Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed to a nonstandard name), it labels the image type as `Unknown`.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Image Attributes window appears with the following information for verification:

Field	Description	Usage Notes
File Name	Filename as it appears in filesystem directory	You cannot add images if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Size of file in bytes.	None.
Image Family	Device family name.	None.
Image Type	Image type, determined from the filename.	Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed to a nonstandard name), it labels the image type as `UNKNOWN`. You must select an image type from an available option before you can add file to repository.
Version	Version of the image	None.
Errors	Click on the link for details.	None.

Step 7 Click **Finish**.

A pop up window appears for you to enter a description.

Step 8 Either:

- Click **OK**.

  The Software Repository Management window appears with the newly added images. The description that you have entered appears in the Comments column in the Software Repository Management window.

  Or

- Click **Cancel**.

  The Software Repository Management window appears with the newly added images. The Comments column in the Software Repository Management window will be blank for this task.

The import from File System may take more time if you have selected many images.

Adding Images to the Software Repository From a URL

Use the following procedure to add software images from a URL to the software repository.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To add images from URL:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management window appears.

Step 2 Click **Add**. Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **URL,** and click **Next**.

The Add Image From URL dialog box appears.

Step 4 Enter the URL details.

For example: http://*servername:portnumber*/file_location

Where,

- *servername* is the name of the server where the image resides.
- *portnumber* is the http port number.
- *file_location* is the image location on the server.

The web server must be running on the destination machine. You can use only HTTP URLs. The remote server should not have any authentication.

Step 5 Click **Next**.

The Job Control Information dialog box appears.

Step 6 Enter the following information in the Job Control Information dialog box:

Field	**Description**
Scheduling	
Run Type	You can specify when you want to run the Image Import (from URL) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 7 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name which you have selected. It also displays the file size of the image.

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Adding Images to the Software Repository From the Network

This option allows you to import running images from all Software Management-supported devices in your network into the software image repository.

Use this option to create a baseline of the image in your network and populate the software image repository. Use the Synchronize report option to review which of the Software Management supported devices are running images that are not in the Software Repository.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You must locate your device in the Supported Image Import Features for Software Management table on Cisco.com. This is because the image baseline capabilities might not be available yet for all devices.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

To add images from network:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from the Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Network**, and click **Next**.

Software Management checks the devices on your network and the software images running on those devices.

To run this check faster, select **Use generated Out-of-sync Report** to find the images that are not in the Software Images repository.

You should generate a Out-of-sync Report before selecting this option. The running images in the network that are not in the Software Repository, appear in the Network Baselining dialog box.

If you have not selected the Use generated Out-of-sync Report option, all running images that are not in the Software Repository appear in the Network Baselining dialog box.

The Network Baselining dialog box contains the following information:

Field	Description
File Name	Filename as it appears in filesystem directory. You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Image size in bytes.
Available at	Location where the image is available on your device.
Error	Click on the link to review the details.

By default, the check boxes of the images that are not in the Software Repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 4 Select/deselect the images and click **Next**.

The Job Control Information dialog box appears.

Step 5 Enter the following information in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Network) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected **Once** for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 6 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name which you have selected. It also displays the file size of the image.

Step 7 Click **Finish.**

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Software Mgmt > Software Mgmt Jobs**.

Synchronizing Software Image Status With Cisco.com

You can check if the software images that are in your software repository are valid images using the Update Status button in the Software Repository Management window.

The Status table column is updated with the following status:

- Not Deferred—Displayed when this image is a valid image.
- Deferred—Displayed when this image is not supported and not available to be downloaded from Cisco.com.

  This image is not recommended by Software Management.
- Software Advisory Notice—Displayed when this image has some issues. You can download this image from Cisco.com.

  This image may be recommended by Software Management. However, you have to read the Software Advisory Notice before importing or upgrading your device.
- Unknown—Displayed when you have added images to the repository for the first time, using any one of these methods:
  - Add Images by Devices
  - Add Images by File system
  - Add Images by URL
  - Add Images from Network

  Use the Update Status button to update the status field.
- Not available—Displayed when information is not available on Cisco.com.

Read the software release notes on Cisco.com for more details.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To synchronize Software Image Status with Cisco.com:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images whose status you want to know and click **Update Status**.

The Cisco.com login dialog box appears.

- If your Cisco.com username and password have not been added to the CiscoWorks database, enter your Cisco.com username and password, click **OK**. If you enter Cisco.com credentials in this workflow then the credentials are valid only for that session.
- If your Cisco.com username and password have been added to the CiscoWorks database, the Cisco.com login dialog box appears with the information that is available in the CiscoWorks database. Click **OK**.

A confirmation message appears that Image Status was retrieved from Cisco.com successfully.

Step 3 Click **OK**.

Review the Status table column in the Software Repository Management window.

Deleting Images From the Software Repository

To delete software images from the software repository:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images that you want to delete, then click **Delete**.

A confirmation message appears, `The selected images will be deleted`.

Step 3 Click **OK**.

The Software Repository Management window reappears after the selected images deleted.

Exporting of Images from Software Repository

To export software images from the Software Repository:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click **Export**.

A confirmation message appears, `The selected images will be exported`.

Step 3 Click **OK**.

The Select directory to export window appears.

Step 4 Click on **Browse** to select a directory to which you want to export the selected image(s).

The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click on OK.

The Image Directory field in the Select directory to export window displays the directory location which you had selected.

Step 6 Click **Next**

A progress bar appears indicating the progress of the export of images.

The Export Image(s) Summary Report appears after completion of the export of the image(s) with these details:

- Number of Selected Image(s)
- Target Directory

- Summary

Step 7 Click **Finish**.

You have successfully exported the image(s) to the selected directory.

Searching for Images From the Software Repository

To search software images from the software repository:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select one of the following from the Filter by drop-down list:

- File Name
- Image Family
- Image Type
- Version
- Size
- Updated At

You cannot use wildcard characters. However, you can filter based on the first character.

For example: If you have images with file names `c3640-i-mz.112-24.P.bin`, `c3640-i-mz.112-25.P.bin`, `cat5000-sup.5-5-18.bin`, and `cat5000-supg.6-4-10.bin`.

If you select File Name as the Filter by option and enter the value as **`c3`**. The filter result displays only `c3640-i-mz.112-24.P.bin` and `c3640-i-mz.112-25.P.bin` images.

Step 3 Click **Filter**.

The Software Repository Management window appears with the filtered image details.

Software Image Attributes

To ensure that Software Management is using the most current information about an image, you should keep the image attributes up to date. Software Management uses image attribute information to:

- Recommend the appropriate image for a given device

  When you distribute an image from the software repository to a device, Software Management uses the image attributes to recommend an image.

- Notify you when a Flash memory or DRAM upgrade is required (upgrade analysis)

When you distribute an image from the Software Repository to a device, Software Management compares the current Flash memory and DRAM attributes with the Flash memory and DRAM requirements for the new image.

The following sections contain:

Understanding Software Image Attributes

To ensure that Software Management is using the most current information about an image, keep the image attributes updated.

If you do not have all the image attribute information when you add the image to the Software Repository, you must edit the attributes when the information becomes available.

Note The auto fill of the Minimum NVRAM, Minimum RAM and Minimum Bootflash image attributes is applicable for IOS only.

See Table 12-5 for the attributes for software images.

Table 12-5 Software Image Attributes

Attribute	Description	Usage Notes
Minimum RAM	Minimum RAM required.	Select it from list of options.
Minimum Flash	Minimum Flash memory required.	Select it from list of options.
Minimum Boot ROM Version	Minimum bootstrap version required.	Enter text in standard Cisco IOS format: a.b(c).
Minimum system software version	Minimum system software version required on the device to upgrade the microcode image (MICA portware, Microcom firmware, CIP microcode only)	Enter text in standard Cisco IOS format: a.b(c).
Minimum supervisor version	Minimum software image version required on supervisor engine module. Cisco Switches can contain any number of modules such as, ATM, FDDI/CDDI, etc. These modules can run different images. There are some interdependencies among the software images that can run on the supervisor engine module and the ATM, FDDI/CDDI, and Token Ring modules residing on the same device chassis.	Enter text in standard Cisco IOS format: a.b(c).
Minimum NVRAM	Minimum NVRAM required to run image on Supervisor Engine III.	Select from list of options.

Understanding Default Attribute Values

The Unknown attribute option has different meanings for different image attributes.

Attribute	Description
RAM	If you select **Unknown**, Software Management computes the RAM value.
Flash size	If Min.Flash is unknown, it is ignored. If the image size is unknown, the required Flash size to copy the image cannot be determined and the image cannot be used for upgrade.
Boot ROM Version	If you select **Unknown**, no value is stored in this field and the image can run with any boot ROM image version.

Finding Missing Attribute Information

When you import an image from another filesystem, the image might not contain all attribute information that Software Management requires.

You can find the missing attribute information in the following ways:

- Read the Release Notes on Cisco.com or the documentation CD-ROM.
- Review the image attribute information that is available along with the images, when you download the images from Cisco.com.

You can update the missing attribute information in the Edit/View Image Attributes dialog box.

See Editing and Viewing the Image Attributes for further details.

Editing and Viewing the Image Attributes

To edit the software images attributes:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click the **File Name**.

The Edit/View Image Attributes dialog box displays attributes for the selected image type.

Step 3 Make your changes in the available editable fields.

For editable image attributes, you will get either a drop-down list or text fields that you can edit.

Step 4 Either,

- Click **Update**. This is if you have updated the image attributes.

  The Software Repository Management dialog box appears after updating the attributes.

  Or

- Click **OK**. This is if you have not updated the image attributes.

  The Software Repository Management dialog box appears without updating the attributes.

Software Distribution

The Software Distribution tab allows you to distribute images in your network and also you can analyze and determine the impact and prerequisites for new software images before distribution.

When you click on the Software Distribution tab, the following options and the entry in the TOC appear:

Options/TOC Entry	Description
Upgrade Analysis (TOC entry.)	You can analyze the image before distribution using: • Cisco.com See Planning an Upgrade From Cisco.com. • Repository See Planning an Upgrade From Repository.
Patch Distribution (TOC entry.)	You can distribute patches to multiple devices using this option. See Patch Distribution.
By devices [Basic] (Option)	Enables you to select devices and then perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image for distribution. See Distributing by Devices [Basic]
By devices [Advanced] (Option)	Enables you to enter the software image and storage media for the device that you want to upgrade. The images that you want to distribute must be available in the Software repository. You can use this method to upgrade the System software on all Software Management supported devices. You can also upgrade module software on any modules that have a management IP address. The modules/interfaces that do not have a management IP address cannot be upgraded using this method. This is for advanced users. See Distributing by Devices [Advanced]
By images. (Option)	Enables you to select a software image from the software image repository and use it to perform an image upgrade on suitable devices in your network. This is useful when you have to distribute the same image to multiple devices. See Distributing by Images
Use remote staging (Option)	Enables you to select a software image, store it temporarily on a device and use this stored image to upgrade suitable devices in your network. This is helpful when the Resource Manager Essentials server and the devices (including the remote stage device) are distributed across a WAN. See Remote Staging and Distribution
Go (Button)	Click this button after selecting the distribution method.

Upgrade Analysis

Before planning an software image upgrade, you must determine the prerequisites of the new software images. You can analyze these by using,

- Cisco.com (See Planning an Upgrade From Cisco.com.)
- Repository (See Planning an Upgrade From Repository.)

You can also launch these tasks for a specific device using the Device Center link from the CiscoWorks LMS Portal home page (**Device Troubleshooting > Device Center**).

Planning an Upgrade From Cisco.com

Use the Cisco.com Upgrade Analysis option to determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.

This option allows you to identify only images that meet certain criteria. It then analyzes the images to determine the required hardware upgrades (boot ROM, Flash memory, RAM, and access).

This option helps you answer such questions as:

- Does the device have sufficient RAM to hold the new software?
- Have` the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Have I performed an upgrade path and NVRAM analysis on my Catalyst devices?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To upgrade from Cisco.com:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

Step 2 Select **Cisco.com** and click **Go**.

The Device Selection dialog box appears.

Step 3 Select the devices to analyze, then click **Next**.

See Using RME Device Selector for information on how to use RME Device Selector.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

   If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

   You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

   Common Services > Security > Cisco.com Connection Management Proxy Server Setup

b. Click **OK** after entering the credential information.

The Cisco.com Upgrade Analysis dialog box appears with the following information:

Field	Description
Device	Name of the device
Running Image	Running image of the device
Image Options	Available images. Select the Image options from the drop-down list.
Error	Click on the link to review the details.

Step 4 Click **Finish** to update the upgrade path information.

The Upgrade Analysis Report appears in a new browser window.

See Understanding the Upgrade Analysis Report for details.

Planning an Upgrade From Repository

Use the Repository Upgrade Analysis option to analyze images in your software repository and determine the impact to and prerequisites for a new software deployment. The option produces the Upgrade Analysis report, which shows the required boot ROM, Flash memory, RAM, and access.

This option helps you answer such questions as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To upgrade from repository:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

Step 2 Select **Repository**, then click **Go**.

The Repository Upgrade Analysis dialog box appears.

Step 3 From the list, select the image to analyze, then select the devices to upgrade, then click **Run Report**.

The Upgrade Analysis Report window appears.

See Understanding the Upgrade Analysis Report for details.

Understanding the Upgrade Analysis Report

The Upgrade Analysis report summarizes the impact to and prerequisites for a new software deployment for the selected devices. It is generated by the Cisco.com Upgrade Analysis (Planning an Upgrade From Cisco.com) and Repository Upgrade Analysis (Planning an Upgrade From Repository) options.

The information that is shown in this report depends on the device type you have selected. See these tables to understand the Upgrade Analysis Report, Table 12-6 and Table 12-7.

Locate your device in the Supported Image Import Features for Software Management table on Cisco.com. For some devices the upgrade analysis option may not be available yet.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baab.html

Table 12-6 Upgrade Analysis Report Columns

Column	Description
Device Information	Running Image Name, Running Image Version, BootROM Version, Running Image Feature, and Device Family
Boot ROM Upgrade	Any boot ROM upgrade required
Flash Upgrade	Any Flash upgrade required
RAM Upgrade	Any RAM upgrade required
Telnet Access	Any Telnet information required
Boot Flash Upgrade	Any boot Flash upgrade required
NVRAM Upgrade	Any NVRAM upgrade required
Module Firmware Upgrade	Firmware upgrade requirements for each service module in device.
Firmware Compatibility	Indicates whether the selected firmware image is compatible with the switch software image running on the device.

The following table (Table 12-7) maps the Upgrade Analysis Report to the supported device types:

- Optical Networking
- Routers
- Switches
- Storage Networking

The Upgrade Analysis from Cisco.com and Repository are not supported for these device types because the required information for the upgrade analysis is not provided by the device:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Security and VPN

- Broadband Cable
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules

Table 12-7 Upgrade Analysis Report Based on Device Type

Upgrade Analysis Report Columns	Device Type: Routers and Optical Networking	Device Type: Switches	Device Type: Storage Networking
Boot ROM Upgrade	Supported	Not supported	Not supported
Flash Upgrade	Supported	Not supported	Not supported
RAM Upgrade	Supported	Supported	Supported
Telnet Access	Supported	Not supported	Supported
Boot Flash Upgrade	Not supported	Supported	Not supported
NVRAM Upgrade	Not supported	Supported	Not supported
Module Firmware Upgrade	Supported. See the Supported Image Distribution Features for Software Management table on Cisco.com for the router's device list that supports Module Firmware Upgrade. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baaa.html	Supported. This is applicable for the following devices: • IPX/IGX/BPX device switch • MGX system	Not supported
Firmware Compatibility	Not supported	Supported. This is applicable for the following devices: IPX/IGX/BPX device firmware	Not supported

In addition to this information, you can use the Go To drop-down list to navigate to particular device analysis report.

Button	Description
Export to File (Icon)	Exports the analysis report in CSV or PDF format.
Print (Icon)	Generates a format that can be printed.

Software Distribution Methods

You can distribute images to the devices in your network, using any of these options:

- Distribute by Devices [Basic]:

  This option enables you to select devices and perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution.

  See Distributing by Devices [Basic]

- Distribute by Devices [Advanced]:

  This option enables you to enter the software image and storage media for the device that you want to upgrade.

  The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you entered when you added devices to the Device Credentials Repository.

  See Distributing by Devices [Advanced]

- Distribute by Images:

  This option enables you to select a software image from the software image repository and use it to perform an image upgrade on suitable devices in your network. This is useful when you have to distribute the same image to multiple devices.

  See Distributing by Images.

- Remote Staging and Distribution:

  This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This is helpful when the Resource Manager Essentials server and the devices (including the remote stage device) are distributed across a WAN.

  See Remote Staging and Distribution.

You can run the device upgrades job sequentially or in parallel. After the devices upgrade, you can also specify the reboot order. You can specify these options in the Job Schedule and Options dialog box.

During the image upgrade, Software Management:

- Checks the amount of Flash memory on the device. If Flash memory needs to be erased before the new system image is loaded and erasing is allowed, it erases the Flash memory. Before erasing the flash, a warning message appears `Flash memory will be erased`.
- Performs MD5 Checksum check of the image when it is downloaded from Cisco.com directly. It also performs image size check once the image is copied to a device, to check if there was any network transfer issue. These are the image consistency checks performed by Software Management.
- Provides a running log of the upgrade job.
- E-mails a report on the results to the specified addresses after completing the upgrade.
- Inserts boot commands to activate the upgraded image.
- Reboots the device if the Reboot Schedule option has been set to Reboot Immediately.
- RAM value is not checked. Hence, distribution proceeds without any errors even if the RAM value is unknown.
- Min.Flash is ignored, if Min.Flash is unknown.
- Image cannot be used for upgrade, if Flash size is unknown.

After you schedule an image upgrade, you can use Software Management Job Browser (**Software Mgmt > Software Mgmt Jobs**) to review, retry, or cancel a job.

After a successful distribution job, Software Management triggers

- A inventory and configuration collection.
- A Change Audit log. You can generate a Change Audit Standard Report in the Report Generator window (**Resource Manager Essentials > Reports > Report Generator**).

Planning the Upgrade

Planning the upgrade typically involves these phases:

- Identifying Possible Changes
- Satisfying the Prerequisites
- Maintaining Your Software Image Repository
- Testing the New Images

Identifying Possible Changes

Identifying which devices at your site might require software upgrades consists of these phases:

- Determine whether an upgrade is required

  You can learn about new features or fixes in different ways.

  You use the Browse Bugs option (**Resource Manager Essentials > Reports > Report Generator > Bug Toolkit**) to summarize the software image bugs for the devices in your network.

  You can schedule a Browse Bugs job to run at regular intervals. This will help you determine any bugs related to current running images on the devices.

  If you find a bug in your software, call the Technical Assistance Center (TAC) to know the status of the bug.

  Your sales engineer or channel partner notifies you of new features that might be appropriate for your site.

  You check Cisco.com periodically to review new release notes, bug-fix documentation, and marketing bulletins.

- Retrieve information about the upgrade

  Go to Cisco.com to read the most recent product Release Notes or bug-fix documentation. This information will help you determine the software image version you need.

- Determine whether the upgrade is really necessary

  After you determine the version you need, you can list the current software version numbers for your managed devices.

  You can generate this using (**Resource Manager Essentials > Reports > Report Generator > Inventory > Software Report**)

Satisfying the Prerequisites

The prerequisites for an software upgrades are:

- Run Cisco.com Upgrade Analysis or Repository Upgrade Analysis to determine the prerequisites for a new software deployment.

  See Upgrade Analysis for further details.

- For IPX/IGX/BPX/MGX devices, you should update upgrade information before running the analysis. Updating upgrade information retrieves the latest upgrade path and firmware compatibility requirements from Cisco.com.

  See Updating Upgrade Information for further details.

In addition, you need to answer such questions as:

- Have you supplied the minimum requirements such as the minimum device configuration requirements for each device? See Meeting Minimum Device Requirements for further details.
- Is the device running from Flash (RFF)?
- Does the device have multiple Flash partitions?
- Does the Supervisor board require a new software image?
- Have you satisfied the additional requirements for the devices?

  See Configuring Devices for Upgrades for further details.

Maintaining Your Software Image Repository

- Use the Adding Images to the Repository > Network option to import running images from all Software Management-supported devices in your network into the repository.

  See Adding Images to the Software Repository From the Network for further details.

- Since you can download new images to a device without using Software Management, eventually the software image repository might not reflect the images that are running on your network devices.

  To keep the repository current:

  - Review all software images in the repository.

    See Software Repository for further details.

  - Schedule the Synchronization report to run periodically.

    See Scheduling a Synchronization Report for further details.

  - Retrieve additional images from Cisco.com, another device, or a file system on your server.

    See Adding Images to the Software Repository for further details.

- Download Cisco images from Cisco.com during a scheduled distribution job.

Testing the New Images

To confirm the stability of your network after upgrades, test the new software images before you perform a full-scale deployment.

You cannot roll back software upgrades for supervisor modules on Catalyst 5000 series switches. Therefore, test the new images for these devices thoroughly before deploying on your network.

Configuring Devices for Upgrades

This section lists all the required tasks that have to be performed on Cisco devices. This section also captures the following information:

- Meeting Minimum Device Requirements
- Meeting Additional Device Requirements
- Additional SFB Checks
- Configuring Telnet and SSH Access
- Configuring SCP
- Configuring rcp
- Configuring TFTP
- Configuring HTTP
- Meeting Microcode and Modem Firmware Requirements

Meeting Minimum Device Requirements

Before you can upgrade software images, you must meet the following requirements:

Category	**Requirements**
Device configuration	Device must be configured with SNMP read-write community string. There should not be any access list on the device that will disable TFTP transfers from the RME workstation.
IOS and ONS devices	For the device to be rebooted using the SNMP protocol, you must configure the **`snmp-server system-shutdown`** command on the device.
SFB devices	See Additional SFB Checks for further details.
RSP 7000 or 7500 devices running Cisco IOS version 11.x or later	See Additional SFB Checks for further details.
Microcode images	See Meeting Microcode and Modem Firmware Requirements for further details.
Inventory	SNMP read-write community string must be in Device and Credentials database (Common Services > Device and Credentials > Device Management).
tftpboot directory space	Must have enough space for all concurrent jobs, which could include image distribution, image import, config file scan, and so on.

Meeting Additional Device Requirements

Before you upgrade, you must meet the following additional device requirements:

- Make sure you have Telnet access to upgrade the devices. Before you upgrade, add the Enable mode password (see Configuring Telnet and SSH Access) and access information for each device to the Device and Credential Repository.

  See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet access.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- To perform the upgrade, the device must be rebooted to RxBoot mode using SNMP. Do this even if you have selected the Do not reboot option when scheduling the upgrade. This is applicable only to RFF devices.
- Configure PIX Firewall for SNMP and telnet access. For RME to manage these devices, you must enter these commands on the device, in the config mode:
  1. **`config terminal`**
  2. **`snmp -server host`** *hostname*
  3. **`snmp -server community`** *community name*
  4. **`telnet`** *ip* 255.255.253.255 *inside interface*
  5. **`write mem`**

Additional SFB Checks

Software Management validates the image upgrades at the time the job is scheduled. For SFB devices, Software Management also verifies that:

- IP routing is enabled on the device.
- The ethernet interface that connects RME to the device has an IP address assigned to it and is routing IP protocol.
- If the device is configured with Frame Relay subinterfaces, the device software version is 11.1 or higher.
- The ROM monitor code version is 5.2 or higher.

Configuring Telnet and SSH Access

Before you schedule the upgrade, use the Device and Credentials (**Common Services > Device and Credentials > Device Management**) option to add or change passwords and access information.

When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2.

If so, it tries to connect to the device using SSHv2.

If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1.

If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2.

If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed.

See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet and SSH access.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- Telnet password

  If the Telnet password is configured on your device, you might need this password for basic login access.

  Enter the Telnet password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- Local user name

  If the device is configured with the local username and password, you must enter this information when log in. In Telnet mode, for catalyst devices, the local user name is not applicable, so you must leave this field blank. In secure shell (SSH) mode, for catalyst devices, you must enter this information.

  Enter the Local User name in the *Primary Credential Username* field in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- Local user password

  If the device is configured with the local username and password, you must enter this information when you log in.

  If TACACS is configured, the application uses the TACACS information.

  If the parent TACACS server is down and the local username and password are present, the application uses this information instead.

  Enter the Local user password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- TACACS username and password

  If the device is configured for TACACS, you must enter the TACACS username and password. The application will try to use this information first for login access.

  Enter the TACACS username and password in the *Primary Credential Username* and *Primary Credential Password* fields in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- Enable secret password

  The enable secret password takes precedence over the enable password in Cisco IOS Release 11.x and later. Use this password to make changes when running in regular Cisco IOS mode. If the service password-encryption is enabled, enable secret passwords are more secure than enable passwords.

  Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- Enable password

  Since some versions of BOOT ROM mode do not recognize the enable secret password or if enable secret is not configured on the device, you must use the enable password to load Flash memory.

  Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Common Services > Device and Credentials > Device Management**).

- Enable TACACS

  Sometimes the device is configured for enable TACACS. In this case, you must provide the TACACS user name and password information for enable access.

  Note The TACACS user name and password must be same as the Local user name and password. You cannot configure different user names and passwords for user mode and enable mode for the device.

Some useful URLs on configuring SSHv2 are:

- Configuring Secure Shell on Routers and Switches Running Cisco IOS:

  http://www.cisco.com/warp/public/707/ssh.shtml

- How to Configure SSH on Catalyst Switches Running Catalyst OS:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a0080094314.shtml
- Configuring the Secure Shell Daemon Protocol on CSS:

  http://www.cisco.com/en/US/partner/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a00801eea45.html#1105358
- Configuration Examples and TechNotes:
  - http://www.cisco.com/en/US/tech/tk583/tk617/tech_configuration_examples_list.html
  - http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802045dc.html

Configuring SCP

You can use the SCP protocol to transfer the software images. While using SCP protocol, the CiscoWorks server acts like a client and the device acts like a server.

To configure a device as a SCP server, see this URL:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html

To configure the CiscoWorks server as a SCP client, you must enter the SSH credentials. See Configuring Telnet and SSH Access for further details.

Configuring rcp

You can use the rcp protocol to transfer the software images. The CiscoWorks server acts like a rcp server and the device acts like a client.

To configure rcp:

- Configuring rcp on Solaris
- Configuring rcp on Windows

Configuring rcp on Solaris

To configure rcp on Solaris:

Creating the rcp Remote User Account

To use rcp, you must create a user account on the system to act as the remote user to authenticate the rcp commands issued by devices. This user account must own an empty.rhosts file in its home directory to which the user, casuser has write access.

You can choose the name of this user account because you can configure the RME server to use any user account.

The default user account name is *cwuser*. The examples in this procedure use the default name *cwuser*. If you choose to use a different name, substitute that name for *cwuser*.

To create and configure the rcp remote user account, follow these steps while logged in as root:

Step 1 Enter:

```
# useradd -m -c "user account to authenticate remote copy operations" \ cwuser
```

Step 2 Navigate to the *cwuser* home directory.

Step 3 Create the .rhosts file, by entering:

```
# touch .rhosts
```

Step 4 Change the owner of the .rhosts file, by entering:

```
# chown cwuser:casusers .rhosts
```

Step 5 Change the permissions of the .rhosts file, by entering:

```
# chmod 0664 .rhosts
```

If you did not use the default user name *cwuser*, use the user account that you created as the rcp remote user account.

a. Log on to the server as admin.

b. Select **Common Services > Server > Admin > System preferences**.

   The View / Edit System Preferences dialog box appears.

c. Enter the name of the user account that you created in the RCP User field, then click **Apply**.

Enabling the rcp Daemon

To add and configure standard Solaris rcp server software:

Step 1 Log in as superuser.

Step 2 Edit the /etc/inetd.conf file using a text editor.

- Look in the file /etc/inetd.conf for the line that invokes rshd. If the line begins with a pound sign (#), remove the pound sign with a text editor. Depending on your system, the line that invokes the rshd server might look similar to:

```
shell   stream   tcp   nowait   root   /usr/sbin/in.rshd   in.rshd
```

- Save the changes to the edited file and exit the text editor.

Step 3 Go to the UNIX prompt, enter the following to display the process identification number for the *inetd* configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root   119   1  0  12:56:14 ?          0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the *inetd* configuration.

Step 4 Enable your system to read the edited /etc/inetd.conf file, enter:

```
# kill -HUP 119
```

where *119* is the process identification number identified in Step 3.

Step 5 Verify that rshd is enabled by entering:

```
# netstat -a | grep shell
```

which should return output similar to:

```
*.shell    *.*     0 0 0 0 LISTEN
```

Configuring rcp on Windows

During CiscoWorks Common Services installation, the rcp server is configured.

Selecting rcp as the Active File Transfer Method on Solaris and Windows:

Step 1 Select **Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences**.

The View/Edit Preferences dialog box appears.

Step 2 Select the **Protocol Order**.

See Selecting and Ordering Protocol Order.

Step 3 Click **Apply**.

Configuring Cisco IOS Software Devices to Allow rcp Transactions

Here is a basic configuration in a router that can handle rcp transactions from the CiscoWorks server.

```
calvi# show running configuration

Building configuration...


Current configuration:

!

version 11.3 service timestamps debug uptime

service timestamps log uptime

service password-encryption

!

hostname calvi

!

boot system c2500-is-l.113-11a.T1.bin 255.255.255.255

enable password 7 1106170043130700

!

username cwuser password 7 000C1C0A05

ip rcmd rcp-enable

ip rcmd remote-host cwuser 172.17.246.221 cwuser enable

ip rcmd remote-username cwuser

!

!

process-max-time 200

!

interface Loopback0

 ip address 5.5.5.5 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0
 description Connection to Backbone
 ip address 172.17.246.4 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip mroute-cache shutdown
 no cdp enable

!
interface Serial1
 no ip address
 no ip mroute-cache shutdown
 no cdp enable
!
interface Async1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.246.1
!
logging monitor informational
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps snmp
snmp-server host 172.17.246.117 traps public

!
line con 0
 exec-timeout 0 0
 password 7 0504080A754D4205
 login
line 1 8
 exec-timeout 0 0
 login
 transport input all
line aux 0
 password 7 06090124184F0515
 login
line vty 0 4
 exec-timeout 0 0
 password 7 06090124184F0515
 login
!
end
```

where:

- `username cwuser password 7 000C1C0A05` creates the username cwuser on the router. You must choose a password for this user.
- `ip rcmd rcp-enable` enables rcp service on the device.
- `ip remote-host cwuser 172.17.246.221 cwuser enable` The remote system where you install CiscoWorks has the IP address 172.17.246.221 and the local definition of the user, cwuser. This command allows cwuser to issue the copy command on the network device.
- `ip rcmd remote-username cwuser` configures use of the remote user name at the request of a remote copy. At the initiation of the remote copy operation in the network device, for example, in Add Images to Library, the device uses the cwuser name to authenticate against the CiscoWorks server.

Configuring TFTP

You can use the Trivial File Transfer Protocol (TFTP) protocol to transfer the software images. The CiscoWorks server acts like a TFTP server and the device acts like a client.

Configuring TFTP on Windows

During CiscoWorks Common Services installation, the tftpboot directory is created under the directory in which RME is installed (the default is *SystemDrive*:\Program Files\CSCOpx).

Configuring TFTP on Solaris

A file transfer server must be installed on your system. You must enable a TFTP server because it is the default file transfer server type.

During Software Management installation, if the installation tool cannot find a TFTP server, it tries to add one. If the installation tool cannot find or create a TFTP server, you must install and enable the TFTP server. Verify that a /tftpboot directory exists, as explained in the following sections.

Enabling the TFTP Daemon

If you are using standard Solaris software, you can add and configure the TFTP server (TFTPD).

Step 1 Log in as superuser.

Step 2 Edit the /etc/inetd.conf file using a text editor.

- Look in the file /etc/inetd.conf for the line that invokes TFTPD. If the line begins with a pound sign (#), remove the pound sign with your text editor. Depending on your system, the line that invokes the TFTP server might look similar to:

  ```
  tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
  ```

- Save the changes to the edited file and exit your text editor.

Step 3 Go to the UNIX prompt, enter the following command to display the process identification number for the inetd configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root  119   1  0  12:56:14 ?           0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the inetd configuration.

Step 4 Enable your system to read the edited /etc/inetd.conf file, enter:

# kill -HUP *119*

where *119* is the process identification number identified in Step 3.

Step 5 Verify that TFTP is enabled by entering either:

# netstat -a

or

# grep tftp

which should return output similar to:

***.tftp Idle**

or enter:

# /opt/CSCOpx/bin/mping -s tftp *localhost_machine_name*

which returns the number of modules sent and received, for example:

```
sent:5 recvd:5 . ..
```

If the output shows that zero modules were received, TFTP is not enabled. Repeat these steps, beginning with Step 1, to make sure you have enabled TFTP.

Creating the /tftpboot Directory

RME uses the /tftpboot directory when transferring files between the RME server and network devices. The files are removed after the transfer is complete. However, multiple jobs (for example, image distribution, image import, or config file scan) could be running at the same time.

Each of these jobs requires its own space. Software image sizes, for example, can be up to 20 MB. To ensure that jobs run successfully, make sure there is sufficient space available in the /tftpboot directory.

If the /tftpboot directory does not exist on your system, you must create it:

Step 1 Enter:

# mkdir /tftpboot

Step 2 Make sure all users have read, write, and execute permissions to the /tftpboot directory by entering:

# chmod 777 /tftpboot

The /tftpboot directory now exists and has the correct permissions.

Configuring HTTP

No configuration on device is required for this protocol.

Meeting Microcode and Modem Firmware Requirements

The following minimum system software versions are required to support microcode and modem firmware upgrades. However, different versions of these image types might require different versions of system software.

Software Management does not check for compatibility and dependence between each microcode version and system software version. It merely warns the user to check this information by consulting a technical representative or the compatibility matrix published on Cisco.com.

MICA Portware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.3(2)T Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.2(9)XA
3640	Cisco IOS version 11.2(12)P

Microcom Firmware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.2(10a)P Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.1(14)AA

CIP Microcode Image Types

Supported for Cisco IOS versions 11.x and later.

Scheduling the Upgrade

Scheduling an upgrade consists of:

- Selecting the devices to upgrade

  Use Software Management's scheduling features to schedule the upgrade for one device or a series of devices.

Software Management downloads images from more than one device in parallel. You must ensure that the tftboot directory (*NMSROOT*/tftboot) has enough free space to accommodate at least 20 images.

- Determining any limitations or requirements for the selected devices

  For example, SFB devices have several upgrade requirements and limitations.

- Updating the inventory

  Since Software Management uses the inventory to make image and Flash memory recommendations, be sure that your current inventory reflects the correct device information.

  For some devices such as 6400 NRP1, 801, and 802, etc., Software Management contacts devices to get the Flash information.

- Configuring file transfer protocol order

  Before scheduling a software upgrade job, set the protocol order for configuration file transfer.

  For fetching configuration from device, the protocol settings of Configuration Management is used. Software Management uses the same protocol for fetch and download of configurations. You can set the Configuration Management protocol order using **Resource Manager Essentials > Admin > Config Mgmt**.

  For better performance, set *tftp* as the first protocol.

- Determining the upgrade and execution order

  Based on your network topology and to minimize the impact on your network, you can schedule the upgrades job either sequentially or in parallel.

  For example, if devices A, B, and C are networked sequentially, then you must upgrade device C first, then device B, then device A. If you upgrade device B first, you might no longer have access to device C.

- Determining the upgrade schedule

  For most devices, you can schedule the software to:

  - Distribute the software to the device and reload the device immediately.
  - Distribute the software only. You will perform the reloads manually.

  The following devices are always rebooted immediately after the software is downloaded:

  - Single Flash bank devices
  - FDDI/CDDI, ATM, and Token Ring modules on Catalyst switches

- Checking the Work Order report

  The Work Order report contains such information as the state of the software running on the device and the new software, the operations that will be performed during the upgrade procedure, and any important notes that you should be aware of before the upgrade begins.

Authorizing a Distribution Job

The Job Approval approval option allows you to require job upgrade approvals before running a scheduled job. It enforces the approval process by sending job requests through e-mail to people on the approver list.

To set up the authorization process:

- Select the appropriate Job Approval options.

- Make sure one or more approver lists exist.
- Make sure the upgrade job identifies an approver list.
- Make sure the approver is a member of that approver list.

See Enabling Approval and Approving Jobs Using Job Approval for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Distributing by Devices [Basic]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

Software Management recommends any software images available on RME server and Cisco.com, if this is option is selected by you (**Admin > Software Mgmt > View/Edit Preferences**).

To do this, select the devices first and distribute suitable images to them. After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

You can also launch this task for a specific device using the Device Center link from CiscoWorks LMS Portal home page.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.

  You can also download the images for the Cisco.com. You must ensure that you have the access to download the images from Cisco.com.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Basic mode:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Basic]** and click **Go**.

The Select Devices dialog box appears.

Step 3 Select the devices, then click **Next**.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Common Services > Security > Cisco.com Connection Management Proxy Server Setup

- Click **OK** after entering the credential information.

The software management analyzes the required images that are available in your software repository and on Cisco.com. It then recommends the appropriate image for distribution.

See Understanding Upgrade Recommendations for details on how Software Management recommends image for various Cisco device types.

The Distribute By Devices dialog box appears with the following information:

Field	**Description**
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Image type, chassis model, and software version on device.
Image Options	Details of the recommended image.
Storage Options	Details of recommended image storage information.
Errors	Click on the underlined Error message to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended image or partition by Software Management. If there is no asterisk at the beginning of the field, it indicates that an appropriate image or partition could not be found but the displayed selections might work.
- A '^' means that the image resides in Cisco.com but not in your software image repository. When you select an image in Cisco.com to distribute to a network device, the image is first added to the image repository, then downloaded to the device.
- A superscript '1' refers to read-only Flash memory.
- A superscript '2' refers to the Flash partition that holds the running image when a device is running from Flash (RFF).

Step 4 Select the devices that you want to distribute images and click **Next**.

The Distribute By Devices window appears with these details:

Field	**Description**
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Image	Image information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS). You cannot select this option, if you have selected the Do not insert new boot commands into configuration file option.
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.

Field	Description
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots
Backup current running image	Select to back up the running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Common Services > Device and Credentials > Device Management) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.

- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Distributing by Devices [Advanced]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you have provided at the time of adding devices to the Device and Credential Repository and the device data that is collected by the RME inventory.

The images that you want to distribute must be available in the Software repository.

You can use this method to upgrade the System software on all Software Management supported devices. You can also upgrade module software on those modules which have a management IP address.

The modules/interfaces that do not have a management IP address cannot be upgraded using this method.

The input file that contains the details of the device and image must be available at this location:

On Solaris:

/var/adm/CSCOpx/files/rme/swim/advdistinput

On Windows:

NMSROOT/files/rme/swim/advdistinput

Where *NMSROOT* is the CiscoWorks installed directory.

After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are present in the image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Advance mode:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Advance]**, then click **Go**.

The Expert Distribution dialog box appears.

Step 3 Click **Browse**.

The Server Side File Browser dialog box appears.

Step 4 Select the file and click **OK**.

The input file that contains the details must be available at this location:

On Solaris:

/var/adm/CSCOpx/files/rme/swim/advdistinput

On Windows:

NMSROOT/files/rme/swim/advdistinput

Where *NMSROOT* is the CiscoWorks installed directory.

The selected file must contain the information in CSV format and all the fields are mandatory:

device-display-name,*image-in-repository*,*storagedestination*,*moduleidentifier*

- *device-display-name*—Name of the device as entered in Device and Credential Repository.
- *image-in-repository*—Image name as in the software image repository.
- *storagedestination*—Image storage destination
- *moduleidentifier*—Module identifier number. This is applicable only for Catalyst devices. For other devices, you must enter 0.

  You can identify the device module number using Inventory Detailed Device Report (**Resource Manager Essentials > Reports > Report Generator**). In the Detailed Device Report, the *Slot Number* column in the *Module Information* table provides you the Module Identifier Number.

For example, for a Cisco Router:

```
Rtr1750,c1700-sy56i-mz.121-24.bin,flash:1,0
```

For a Cisco Catalyst device:

```
cat5500-10.100.38.17,cat5000-supg.6-4-10.bin,bootflash:,1
```

Step 5 Click **Verify**.

The Expert Distribution window is updated with the following device details:

Field	Description
Device	Name of the device as specified in the input file.
Image	Name of the image as specified in the input file.
Storage Destination	Image storage information as specified in the input file.
Module Number	Module identifier number as specified in the input file.
Result	Click on the link to review the details.

Step 6 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 7 Enter the following information in the Job Schedule and Options dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Advance]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	

Field	Description
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Applies to Supervisor Engine I, II, and III only. Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated. • Applies to Supervisor Engine III only.
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: • Applies to Supervisor Engine I, II, and III only. • Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots
Back up current running image	Select to back up the running image in software image repository before upgrading. Applies to Supervisor Engine I, II, and III only. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.

Field	Description
Enable Job Password	Enter the password for the distribution job. This password is used to Telnet to the devices at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Common Services > Device and Credentials > Device Management) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 8 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Distributing by Images

You can use the Distribute by Images option to schedule image-centric upgrade jobs. To do this, you must first select an image and then distribute it to applicable devices.

After the distribution job is complete, you can use the Job Details report to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You cannot use this procedure to upgrade:

- MICA portware
- Microcom firmware
- CIP microcode
- Bootloader for IOS
- Catalyst modules other than the Supervisor module

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are in the image repository.

  See Planning the Upgrade for further details.
- Considered the effect of the upgrade on your network and your network users.

  See Scheduling the Upgrade for further details.
- Supplied the information required by Software Management for each device.

  See Configuring Devices for Upgrades for further details.

To distribute images by image:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By image**, then click **Go**.

The Select Image And Devices dialog box appears.

Step 3 Select:

a. An image from the software image repository.

b. Devices that need upgrading

Step 4 Click **Next**.

The Device Recommendation dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Image type, chassis model, and software version on device.
Recommended Storage	Details of recommended image storage information.
Error	Click on the link to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended partition by Software Management. If there is no asterisk at the beginning of the field indicates, an appropriate partition could not be found but the displayed selections might work.
- A superscript '1' refers to read-only Flash memory.

Step 5 Select the devices you want to upgrade, then click **Next**.

The Image Centric Distribution Verification window appears. This window displays the following information:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Software management recommends the Flash partition with the maximum free space in each device. You can override the recommendation and select another partition from the drop-down box.

Step 6 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 7 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by image) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.

Field	Description
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.

Field	Description
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Common Services > Device and Credentials > Device Management) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 8 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your job, select **Software Mgmt > Software Mgmt Jobs**.

Support for IOS Software Modularity

Software Management provides support for Cisco IOS Software Modularity Images. The Cisco IOS Software Modularity Images combine subsystems into individual processes and enhances the memory architecture in order to provide the process level fault isolation and subsystem In-Service Software Upgrade(ISSU) capability.

Traditionally, IOS Software images are distributed by:

- Copying the image to disk.
- Updating boot commands and rebooted.

The IOS Software Modularity images can be run in this mode as well, this is called Cisco IOS Software Modular non-install mode (also known as binary mode).

Software Management supports distribution of Patches and Maintenance Packs. This is accomplished by the use of Cisco IOS Software Modularity Images. Software Modularity enhances the IOS infrastructure to allow selective system maintenance through individual patch upgrades. See Patch Distribution for more details.

Patches

A patch is a single fix which may affect one or more subsystems. Patches can only be installed to a search root, where a base image exists. Patches are released for a particular base image version and device platform.

Maintenance Pack

A Maintenance Pack includes one or more patches. This is applied like a Patch. Maintenance Packs are released for a particular base image version and device platform.

Note Software Management does not support downloading Patches/Maintenance Packs from Cisco.com. The reason is these images are available in external URL. You have to manually download patches from the external URL and add the same to Software Repository.

Modes of Distribution

There are two modes of distribution of Software Modularity images to devices:

- **Non Installed Mode:** This process involves the distribution of images by copying of the IOS Software Modularity images to the hard disk of the device, updating the boot commands and rebooting the OS on the device. You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.
- **Installed Mode:** According to this mode the IOS Software Modularity image is extracted/uncompressed to a compact flash with a well defined directory structure. The installed mode provides the advantage of accomodating the point fix capabilities of Software Modularity.

Note Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution. Software Management only recommends Maintenance Pack Images for devices. It does not recommend patches for devices.

Cisco IOS Software Modularity base images support:

- Import of Image from Cisco.com
- Import of Image from device
- Import of Image form File System
- Import of Image from Network
- Cisco.com Upgrade Analysis
- Distribution of Images
- Software Repository Synchronization

Support for Import of Image from device, Import of Image from Network and Software Repository Synchronization is only applicable for devices running IOS Software Modularity images in non-installed mode.

The population of Flash files on Cisco-Flash-MIB is not done on the devices running IOS Software Modularity image versions 12.2(18)SXF4 and 12.2(18)SXF5 and so these image versions are not supported by Software Management. The minimum IOS Software Modularity image version supported by Software Management is 12.2(18)SXF6

Patch Distribution

You can distribute patches simultaneously to applicable devices. Patch distribution does not require reboot of the entire OS on a device. You can install a patches only to a search root where a base image exists. Patches, once installed, must be activated to come to effect on the running system.

Note You can apply Patches or Maintenance Packs to a device only if the device is running IOS Software Modularity Images in installed mode.

Software Management verifies:

- Patches against the base image and device platform to ensure compatibility. If the patches are incompatible then those patches are rejected.
- Whether the target patch already exists on the device.

Patch Distribution Methods

You can distribute patch images to the devices in your network, using any of these methods:

- **Distribute by Devices**

  This method enables you to select devices and perform patch upgrades to those devices.

  See Patch Distribution - by Devices.
- **Distribute by Patch**

This method enables you to select a patch image from the Software Repository and use it to perform a patch upgrade on suitable devices in your network. This is useful when you have to distribute the same patch image to multiple devices.

See Patch Distribution - by Patch.

Patch Distribution - by Devices

You can use the Distribute by Devices option to schedule device-centric patch upgrade jobs.

Software Management recommends any Maintenance Pack software images available in RME Repository.

Note Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution> Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By devices** and click **Proceed**.

The Patch Distribute by Devices dialog box appears. The Device Selector lists all the available devices.

Step 3 Select the devices, then click **Next**.

If any of the selected device is not in install mode, an error message is displayed:

```
Device is not in installed mode or not patchable
```

Deselect the device that is not in installed mode and continue.

The software management analyzes the required patch images that are available in your software repository and lists the applicable patch images for each device selected. You can select one or more required patches from the list for each device by using the Ctrl key.

You should select atleast one patch for each selected device. If you do not select a patch for a device, an error message is displayed.

```
You should select atleast one patch image for each selected device.
```

Ensure that you select atleast one patch for each selected device and continue.

The Patch Distribute By Devices dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Patch type, chassis model, and software version on device.
Patches Options	Details of the patch.
Storage Location	Details of of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Patch Distribute By Devices window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Patch	Patch information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs.	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.

Field	Description
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Patch Distribution - by Patch

You can use the Distribute by Patch option to schedule patch upgrade jobs.

Note Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See Adding Images to the Software Repository From a File System for more details..

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution> Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By Patch** and click **Proceed**.

The Distribute by Patch dialog box appears.

Step 3 Select a patch from the Image Selection pane and devices from the Device Selection pane,and click **Next**.

The Distribute By Patch - Recommendations dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Distribute By Patch - Verification window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do *not* select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.

Field	Description
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click **Done**.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Remote Staging and Distribution

The Remote Staging and Distribution option helps you to upgrade multiple devices over a WAN.

You can perform remote staging and distribution by either of the methods:

- External TFTP server
- Remote Staging Device

In this workflow, a managed device or external TFTP server is used to stage an image temporarily. The staged image is then used to upgrade devices that are connected by LAN to the Remote Stage device or external TFTP server. This saves you from copying a similar image, multiple times across the WAN.

After the image distribution job is completed using a managed device as a remote stage device, the configuration changes made to the Remote Stage device are automatically reversed and the staged image is deleted from the Remote Stage device.

After the distribution job is complete, you can use the Software Mgmt Jobs tab to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Supported Remote Stage Devices

The device that is used as the Remote Stage must have enough free flash space to copy the selected image.

See the Supported Image Distribution Features for Software Management table on Cisco.com for Remote Staging devices list.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a008055baaa.html

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device or external TFTP server. You should also verified whether the necessary software images are in the image repository.
- Manually copied the software image to the External TFTP Server in case you are using the External TFTP server as the Staging Server.
- Considered the effect of the upgrade on your network and your network users.
- Supply the necessary information required by Software Management for each device.
- Decide on the device or external TFTP server that you will use as the Remote Stage device or server.

To distribute images using Remote Staging:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **Use remote staging** and click **Go**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select either:

- **Using External TFTP Server** to use an external TFTP server as the staging server.

  or

- **Using Remote Stage Device** to use a device as the remote staging device.

If you have selected Using Remote Stage Device option, go to Step 4.

If you have selected Using External TFTP Server option, go to Step 9.

Step 4 Go to the Select Remote Stage Device pane, select a device that you want to use as the remote stage device. Ensure that you select a device that supports remote staging.

If you select a device that does not support remote staging, an error message is displayed.

Step 5 Click **Next.**

The Remote Staging and Distribution dialog box appears.

Step 6 Select:

a. An image from the Image Selection pane.

b. Either click on **Select Applicable Devices** button to automatically select the applicable devices or manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 7 Click **Next**.

The Remote Stage and Image Upgrade Details dialog box appears with the following details:

Field	Description
Remote Stage Name	Name of the remote stage device that you want to use as a remote stage.
Selected Image	Image name that you have selected for distribution.
Storage Options	Image storage information

Step 8 Click **Next**.

If the Remote Stage verification fails, check if the Remote Stage device has enough free space and restart the procedure from Step 3.

The Device Recommendation dialog box appears. This displays the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.

After the above step, go to Step 14.

Step 9 If you have selected the**Using External TFTP Server** option enter the external TFTP server IP address in the Enter TFTP IP Address text box.

Step 10 Click **Next.**

The Remote Staging and Distribution dialog box appears.

Step 11 Select:

a. An image from the Image Selection pane.

b. Either click on **Select Applicable Devices** button to automatically select the applicable devices or manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see Unsupported Software Images.

Step 12 Click **Next**.

The External TFTP Server Details dialog box appears with the following details:

Field	Description
IP Address	IP Address of the External TFTP server.
Selected Image	Image name that you have selected for distribution.
Errors	Error information.

Step 13 Click **Next**.

The Device Recommendation dialog box appears with the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Device Center.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.
Errors	Error information.

Step 14 Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 15 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 16 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.

Field	Description
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Field	Description
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: • This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. • Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do *not* select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Common Services > Device and Credentials > Device Management) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See Viewing/Editing Preferences for more details.

Field	Description
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: 1. Click **Execution Order**. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click **Done**.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: 1. Click **Boot Order**. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click **Done**.

Step 17 Click **Next** after you finish entering the job information details

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP server.
- Verification warnings generated during image distribution (if applicable).

Step 18 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Software Mgmt > Software Mgmt Jobs**.

Unsupported Software Images

During remote staging, there maybe software images running on the devices selected for remote staging, but some of them may not get listed as available images. This is because, some software images do not support Remote Staging and Distribution.

The below table lists the software images that do not support Remote Staging and Distribution.:

Unsupported Software Images
CSS_SW FDDI_CDDI
ATM_WTALL
ATM_WBPVC
CIP
CSS_11000_SW
C6KMODULE_MWAM_SW
PATCH_SW
ONS15530
TOKENRING
ATM_WBLANE
BOOT_LOADER
C6KMODULE_MWAM_SW
CSS_11500_SW
CSS_11000_SW
C2500
C1600
BLADERUNNER
ATM_WTOKEN
MICA MICROCOM
NAM_APPL_SW
SPA_FPD_SW
CSS_11500_SW
ONS15540

Understanding Upgrade Recommendations

This section describes how Software Management recommends image for the various Cisco device types:

- Upgrade Recommendation for Cisco IOS Devices
- Upgrade Recommendation for Catalyst Devices
- Upgrade Recommendation for VPN 3000 Series
- Upgrade Recommendation for Catalyst 1900/2820
- Upgrade Recommendation for Other Device Types

Upgrade Recommendation for Cisco IOS Devices

To determine the recommended software images for Cisco IOS devices, Software Management:

1. Lists all images in the software repository that can run on the device. For example, C7000 images run on 7000 and 7010 devices, IGS images run on 25xx devices, and so on.
2. Removes all listed images that require:
    - More RAM or Flash memory than is available on the device.
    - A newer boot ROM than the one on the device.

    If RAM is UNKNOWN, it is not considered in any comparison operation (image filtering). However, you are warned during the subsequent task.
3. Recommends an image whose feature subset matches the image running on the device.
    - Any images that support all current features and include some additional ones, take precedence over images that match exactly.
    - If more than one image is either a superset or an exact match of the running image, the latest version takes precedence over earlier versions.
4. Removes the images from recommendation if the images Min.Flash size requirement is not met by the device.

    If Min.Flash required is UNKNOWN, it is not considered in any comparison operation (image filtering).

    If Flash Size is UNKNOWN, the image cannot be used for upgrade.

    See the IOS Software Release documentation on Cisco.com to know the Min.Flash size.
5. Depending on the image feature list, Software Management recommends an image whose image version is lower than the current running image version.
6. Recommends to filter out the images that are larger in size than the flash available on the device.
7. Recommends Flash partitions on the device along with the storage details, if you are upgrading the Boot Loader image.

This algorithm might recommend images that are older than the one running on the device.

To ensure that only newer images are recommended, select **Admin > Software Mgmt > View/Edit Preferences**. In the View/Edit Preferences dialog box, select the Include images higher than running image checkbox, then click **Apply**.

Upgrade Recommendation for Catalyst Devices

For Catalyst device upgrades, Software Management typically recommends the latest version images in the software repository.

For default RAM requirements for Supervisor Engine I and Supervisor Engine III, however, Software Management uses:

Module Type and Version	Default RAM (MB)
Supervisor Engine III	32
Supervisor version 2.1 up to (but not including) 3.1	8

Module Type and Version	Default RAM (MB)
Supervisor version 3.1.1 and later	16
Maintenance release versions 3.1 and 3.2 with "Sup8M" in filename	8

For supervisor versions 3.1 to 3.2, when the image repository or Cisco.com has both 8 MB of RAM and regular images available, Software Management also checks the device RAM:

1. If the RAM can be determined and the available RAM is greater than 16 MB;

a. Software Management recommends the latest regular supervisor image where the RAM requirement is less than the available RAM.

b. If no regular image with matching RAM requirements is available, it recommends the latest version of the 8-MB images.

c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

2. If the RAM can be determined and the available RAM is less than 16 MB:

a. Software Management recommends the highest image version for which the RAM requirement is less than 16 MB.

b. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

3. If the RAM cannot be determined:

a. Software Management recommends the latest regular image.

b. If no regular image is available, it recommends the latest 8-MB image.

c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

The minimum RAM in the image attributes file supersedes these guidelines.

For example, if a supervisor engine module is running the version 3.1 maintenance release (8 MB RAM) but the RAM in the image attributes was changed to 16 MB, Software Management uses the value in the attributes file.

Upgrade Recommendation for VPN 3000 Series

Software Management recommends the latest version of the image in the software image repository. If the device is a VPN 3005 Concentrator, it recommends the VPN 3005 System software images in the repository.

Upgrade Recommendation for Catalyst 1900/2820

For Catalyst 1900/2820 Enterprise version device upgrades, Software Management typically recommends the latest version of images in the software repository.

Note For Catalyst 1900/2820 Series devices, Software Management recommends images with version numbers greater than 8.0(0) because the older versions do not support the Command Line Interface. Non-Enterprise versions of the Catalyst 1900/2820 are not supported in Software Management.

Upgrade Recommendation for Other Device Types

For the following device types, Software Management recommends the latest version of the image in the software image repository:

- PIX Firewall Devices

  If you are running PIX image version 7.0 or later, while recommending the image, Software Management will also recommend the storage details of the device.
- Content Service Switches
- Aironet AP Series
- Optical Switch Series
- Network Analysis Module Series
- Content Engines

Using Software Management Job Browser

Using this window you can view all your scheduled Software Management jobs.

The Software Management Job Browser contains the following fields and buttons:

- Software Management Job Browser Fields(Table 12-8)
- Software Management Job Browser Buttons (Table 12-9)

The Software Management Job Browser displays the following details for a job:

Table 12-8 Software Management Job Browser Fields

Field	Description
Job ID	Unique number assigned to the job when it is created. Click to display a summary of job details and schedule options. See Understanding the Software Management Job Summary for further details.
Job Type	Type of job such as Import Images, Distribute Images.

Table 12-8 Software Management Job Browser Fields (continued)

Field	Description
Status	Job states: • Successful—Job completed successfully • Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed amounts to 5. • Running—Job still running. • Pending—Job scheduled to run. • Stopped—Running job stopped by you. • Missed Start—Job could not run for some reason at the scheduled time. For example, if the system was down when the job was scheduled to start, when the system comes up again, the job does not run. This is because the scheduled time for the job has elapsed. The status for the specified job will be displayed as “Missed Start”. • Approved—Job approved by an approver • Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details. • Waiting for Approval—Job waiting for approval.
Description	Job description as entered at the time of creation.
Owner	User who created the job.
Scheduled At	Start time of the scheduled job.
Completed At	End time of the scheduled job.
Schedule Type	Type of the scheduled job: • Immediate • Once

Table 12-9 Software Management Job Browser Buttons

Buttons	Description
Edit	Reschedules the job. You can change the schedule only for jobs that are either in the Pending, Waiting for Approval or the Approved status. See Changing the Schedule of a Job.
Retry	Retry the failed job. You can retry only failed distribution jobs. See Retry a Failed Distribution Job.

Table 12-9 Software Management Job Browser Buttons (continued)

Buttons	Description
Undo	Undo a successful job. You can undo only successful distribution jobs. See Undo a Successful Distribution Job.
Stop	Stops a scheduled job. You can Stop only jobs that are either in the Pending or the Running status. See Stopping a Job.
Delete	Delete the jobs. See Deleting Jobs.
Refresh (Icon)	Click on this icon to refresh the Software Management Job Browser Window.

Changing the Schedule of a Job

You can change the schedule only for jobs that are either in the Pending, Waiting for Approval or the Approved status.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To change the schedule of a job:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or an approved job.

Step 3 Click **Edit**.

The Change Job Schedule dialog box appears.

Step 4 Change the schedule.

Step 5 Click **Submit**.

Retry a Failed Distribution Job

You can retry only failed distribution jobs.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To retry a Job:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a failed distribution job.

Step 3 Click **Retry**.

The Retry Upgrade dialog box appears with the following information:

Field	Description
Device Information	Name of the device
Module	Device module
Pre-upgrade Image	Image name which was running before the upgrade.
Selected Image	Image name that is selected for distribution.
Running Image	Image name that is currently running on the image.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution depending on your previous distribution selection:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution

Undo a Successful Distribution Job

You can undo only successful Distribution jobs.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To undo a job:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a successful distribution job.

Step 3 Click **Undo**.

The Undo Upgrade dialog box appears with the following information:

Field	Description
Device	Name of the device
Module	Device module
Pre-upgrade Image	Image name which was running before the upgrade.
Post-upgrade Image	Image name after completing the upgrade.
Running Image	Image name that is currently running on the image.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution. This depend on what you selected earlier in the Distribution Method window:

- Distributing by Devices [Basic]
- Distributing by Devices [Advanced]
- Distributing by Images
- Remote Staging and Distribution

Stopping a Job

You can stop only jobs that are either in the Pending or the Running status.

The job stops only after the current task is complete. During this time, the Software Management Job Browser window displays the job status as Running.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To stop a job:

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or a running job.

Step 3 Click **Stop**.

A confirmation box shows that the selected job will be stopped.

Step 4 Click **OK**.

A message appears that the selected job has been stopped.

After the job is stopped, the Pending job status changes to Stopped. The Running job status changes temporarily to Stop Initiated and then to Stopped.

Deleting Jobs

To delete jobs:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select the jobs.

Step 3 Click **Delete**.

A confirmation box shows that the selected jobs will be deleted.

Step 4 Click **OK**.

Understanding the Software Management Job Summary

From the Software Management Job Browser, you can learn more about one job by viewing its details. You can view this details by clicking the Job ID on the Software Management Job Browser window.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

The Software Management Job Details window contains the following information:

Page/Folder	Description
Work Order	Select a device to view the summary of the job: • If there is more than one device, the software distribution order. • The state of the running image on the device. • The image selected for the upgrade. • Whether Flash memory will be erased before the new image is loaded. • Operations that will be performed during the upgrade procedure. • For a bootloader upgrade, whether the bootloader will be upgraded. • The Job Approval information. • Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device. • Details of the Remote Stage device (if applicable). • Verification warnings generated during image distribution (if applicable).

Page/Folder	Description
Job Results	Select a device to view the complete job result. It displays information on: • The job status, start time and end time. • The job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully. • The import/upgrade mode (parallel or sequential) • The protocol order used for image transfer and configuration tasks. • How the job was processed.
Summary[On Job Complete]	Displays the summary of the completed job For software distribution jobs, the summary contains details about the device, image type, running image name, upgrade image name, upgrade storage location, and image distribution status. For software import jobs, the summary contains details about device, image name, storage location, and import status of the image. The Job Summary is not generated for Image Out-Of-Sync Report job.

Understanding User-supplied Scripts

User-supplied scripts are run before and after each device upgrade, for example:

- The preupgrade script can check whether the device is accessible.
- The preupgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before upgrading.
- The post-upgrade script can check whether the upgrade was successful. Depending on the return value, Software Management either halts or continues with the rest of the upgrade.

The following sections contain:

- Script Requirements
- Script Parameters
- Sample Script

Script Requirements

- In the Edit Preferences dialog box (**Admin > Software Mgmt > View/Edit Preferences**), enter:
  - Enter the shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows.

    On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission.

    On Windows, the script should have read, write, and execute permissions for casuser/Administrator.

    The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the *casuser* account.
  - The script files *must* be available at this location:

    On UNIX:

/var/adm/CSCOpx/files/scripts/swim

On Windows:

NMSROOT/files/scripts/swim

  - User script timeout

    Software Management waits for the time specified before concluding that the script has failed.

- Software Management verifies that:
  - The script has write and execute permissions for the user *casuser*.
  - Only users logged in as Administrator, root, or *casuser* have write and execute permissions.

Caution The script should not write output to the system console. The script can write the output to a file. Writing the script output to the system console can cause the Software Management job to hang.

Script Parameters

Software Management passes a parameter indicating whether the script is running before or after the upgrade. If the script does not intend to perform any pre-upgrade check, the script can return an exit value of zero and perform checks in the post-upgrade. See the Sample Script for reference.

The parameters provided to the script by Software Management are in the form of environment variables.

The server environment variables such as *PATH*, *SystemRoot*, etc., are not passed on to the script by Software Management. You have to set the relevant environment variables within the script. See the Sample Script for reference.

See Adding Devices to the Device and Credential Repository section in the Common Services User Guide and Online Help for further information on device hostname, device name (device display name), SNMP v2 community strings, etc.

The different parameters are described in the table below:

Variable	Description
CRM_SCRIPT_CONTEXT	This variable is used to determine if the script has to be invoked before or after image upgrade. If you set the variable to, • PRE-DOWNLOAD—Script is invoked by Software Management prior to image upgrade. • POST-DOWNLOAD—Script is invoked by Software Management post image upgrade.
NMSROOT	CiscoWorks installed directory.
TMPDIR	Directory provided to CiscoWorks to create temporary files.
CRM_DEV_NAME	Name of Device Display name as entered in Device and Credential Repository.
CRM_SNMP_V2_RWCOMMUNITY	SNMP version 2 read-write community string.
CRM_SNMP_V2_ROCOMMUNITY	SNMP version 2 read only community string.
CRM_SNMP_V3_ENGINE_ID	SNMP version 3 Engine ID
CRM_SNMP_V3_USER_ID	User ID configured for SNMP version 3 protocol access on the device.
CRM_SNMP_V3_PASSWORD	SNMP version 3 password for the user ID.

Variable	Description
CRM_ENABLE_PASSWORD	Enable password.
CRM_PRIMARY_USERNAME	Primary user name configured on the device.
CRM_PRIMARY_PASSWORD	Primary password configured on the device.
CRM_DEV_MGMT_IP_ADDR	IP address provided in Device and Credential Repository for management.

Sample Script

The sample script illustrates how to use this option before the upgrade to see if the device is accessible and after the upgrade to see whether it was successful.

The *sample.bat* file contains:

```
c:\progra~1\cscopx\bin\perl c:\progra~1\cscopx\files\scripts\swim\samplescript.pl
```

The *samplescript.pl* file contains:

```
#!/usr/bin/perl
BEGIN
{
use lib "$ENV{NMSROOT}/objects/perl5/lib/Net";

}
use Net::Telnet;
#my $output="";
## The following Environment variables are not passed on by Software Image Management
## Need to set these variables for the script to work as expected
$ENV{'Path'}="C:\\PROGRA~1\\CSCOpx\\MDC\\tomcat\\bin;C:\\PROGRA~1\\CSCOpx\\MDC\\Apache;C:\\PROGRA~1\\CSCOpx\\
MDC\\jre\\bin;C:\\PROGRA~1\\CSCOpx\\MDC\\bin;C:\\PROGRA~1\\CSCOpx\\lib\\jre\\bin\\server;C:\\PROGRA~1\\CSCOpx
\\objects\\db\\win32;C:\\PROGRA~1\\CSCOpx\\bin;c:\\cscopx\\lib\\jre\\bin\\server;c:\\cscopx\\lib\\jre141\\bin
\\server;C:\\WINNT\\system32;C:\\WINNT;C:\\WINNT\\System32\\Wbem;C:\\Program Files\\Common Files\\Adaptec
Shared\\System;c:\\progra~1\\cscopx;c:\\progra~1\\cscopx\\bin;";
$ENV{'TEMP'}=$ENV{'TMPDIR'};
$ENV{'TMP'}=$ENV{'TMPDIR'};
$ENV{'SystemRoot'}="C:\\WINNT";
######  Required Environment variables are set #########
my $prmptchar = '/\>/i';
$filename = $ENV{'CRM_DEV_NAME'} . '.txt';
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq  'PRE-DOWNLOAD') {
open OUTFILE, "> $filename" or die "Can't open file";
print OUTFILE %ENV;

my $host = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwd = $ENV{'CRM_PRIMARY_PASSWORD'};
print OUTFILE $host;
print OUTFILE $pwd;
$telnet = new Net::Telnet(Input_Log=>"inp.txt");
$prev = $telnet->host($host);
print OUTFILE $prev;
print OUTFILE "Conntecting to Host....";
$telnet->open($host);
print OUTFILE "Connected ...";
$telnet->dump_log("dmp.txt");
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwd);
print OUTFILE "Password send";
($output) = $telnet->waitfor('/#$/i');
print OUTFILE "Returned after waitfor";
print OUTFILE $output;
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($output) = $telnet->waitfor('/#$/i');
print OUTFILE $output;
### If the device is not running the expected Image, return 1
### so that Software Image Management application does not proceed.
if ($output =~ m/Version 12.2\(27\)/) {
    print OUTFILE "Required Software running on Device, Allow to proceed with Upgrade\n"

    }
else
    {
    print OUTFILE "Upgrade stopped, Device not running desired Image";
    close OUTFILE;
    exit(1);
    }
close OUTFILE;
## A return vale of zero(0) allows the Software Image Management application to proceed
exit(0);
}
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq  "POST-DOWNLOAD") {
my $hostnew = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwdnew = $ENV{'CRM_PRIMARY_PASSWORD'};
open OUTFILE, ">>$filename" or die "Can't open file";
print OUTFILE "====== POST DOWNLOAD RESULTS ========";
$telnet = new Net::Telnet(Input_Log=>"inp1.txt");
$telnet->dump_log("dmpo.txt");
$telnet->open($hostnew);
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwdnew);
($opt) = $telnet->waitfor('/#$/i');
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($opt) = $telnet->waitfor('/#$/i');
if ($opt =~ m/Version 12.3\(10a\)/) {
    print OUTFILE "Required Software running on Device, Upgrade Successful\n";
}
print OUTFILE $opt;
close OUTFILE;
exit(0);
}
```

Locating Software Management Files

This table shows the locations of some of the Software Management directories and log files that describe what is happening in the system.

Contents	Operating System	Location
Software Management User Interface/job creation debug log file	UNIX	/var/adm/CSCOpx/log/swim_debug.log
	Windows	*NMSROOT*/log/swim_debug.log Where *NMSROOT* is the CiscoWorks installed directory.

Contents	Operating System	Location
Software Management job execution debug log files. You can set the debug mode for Software Management application in the Log Level Settings dialog box (Resource Manager Essentials > Admin > System Preferences > Loglevel Settings	UNIX	/var/adm/CSCOpx/files/rme/jobs/swim/*job-id*/swim_debug.log
	Windows	*NMSROOT*\files\rme\jobs\swim\job-id\swim_debug.log Where *NMSROOT* is the CiscoWorks installed directory.

CHAPTER 13

Tracking Network Changes Using Change Audit

Change Audit tracks and reports changes made in the network. Change Audit allows other RME applications to log change information to a central repository. Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit.

RME applications write change records to Change Audit. Change Audit stores these records in the log tables (summary and details) for later use with reports.

For example, Software Management records a change for each completed device upgrade. If a job has ten devices, then Software Management writes ten entries to the Change Audit log, but the Change Audit report shows only one job with ten devices. You can then access individual device information.

Each application writes its own change records to Change Audit. For example, in Inventory you can set inventory change filters to filter out all kinds of information for different device types. Change Audit record maintenance is controlled by the Change Audit Delete Change History option.

You can convert change records into SNMP V1 traps and forward them to a destination of your choice. This allows system administrators to forward critical network change data to their own NMS.

You can define automated actions (e-mail and automated scripts) on creation of change audit record. The automated action gets triggered on creation of the change audit record.

How Does it Differ From Syslog?

Syslog clients or message suppliers are Cisco devices that have been configured to log messages to RME. Syslog Analyzer receives messages from routers and other Cisco devices configured to send messages to the syslog server in RME. The messages are sent either directly or through a remote syslog collector installed in the network. These messages originate from the device in response to some activity that affects it.

Change Audit clients are RME applications that record change information. Applications, such as Software Management, send messages to Change Audit when they make a change to the network, for example, uploading a new Cisco IOS image.

Often these changes and users who make changes from the command line interface also trigger syslog messages. The messages are logged in the RME syslog facility and are also passed on to other RME applications for processing.

For example, a device sends a syslog message about a device configuration change. This is passed on to Device Configuration, which determines the exact nature of the change and then writes a change record into the Change Audit log.

Performing Change Audit Tasks

Change Audit allows you to:

- Determine changes being made in the network during critical operations time

  System administrators can define the start and end times during the day when network changes should not be made. Based on this selection you can quickly see, for a given day, whether changes were made when they should not be.

  See Defining Exception Periods for defining the exception periods.

- Define automated actions on creation of change audit record

  Automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are, E-mail, Traps, and Automated scripts

  See Defining Automated Actions for defining the Change Audit automated actions.

- Monitor your software image distribution and download history for software changes made using the Software Management application.

  Software Management automatically sends network change data to the Change Audit summary and details tables.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- Track any configuration file changes

  Device Configuration automatically sends data on configuration file changes to the Change Audit log.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- Monitor inventory additions, deletions, or changes

  Inventory tracks specific messages or monitors any and all changes in your network inventory. To set inventory filters, use the Inventory Change Filter option.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- View all the latest changes that occurred in the network over the last 24 hours

  24-Hour Reports provides a quick way to access the latest changes in the Change Audit log.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- Purging the Change Audit records

  Frees disk space and maintains your Change Audit records at a manageable size. You can either schedule for periodic purge or perform a forced purge of Change Audit data.

  See Performing Maintenance Tasks for scheduling a periodic purge.

- Generating change audit data in XML format

  `cwcli export changeaudit` is a command line tool that also provides servlet access to change audit data. This tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.

  See Overview: cwcli export Command for generating the Change Audit data in XML format.

- Set the debug mode for Change Audit application

You can set the debug mode for Change Audit application in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

- Using Device Center you can perform the following Change Audit tasks:
  - Generate the 24-hour Change Audit Summary report for a selected device.
  - Generate the Change Audit Standard report for a selected device.

  See RME Device Center for further information.

For the new features in this release, see What's New in this Release.

Performing Maintenance Tasks

You can either schedule for periodic purge or perform a forced purge of Change Audit data. This frees disk space and maintains your Change Audit data at a manageable size.

You can perform these tasks using the **Resource Manager Essentials > Admin > Change Audit** tab:

- Setting the Purge Policy
- Performing a Forced Purge
- Config Change Filter

Setting the Purge Policy

You can specify a default policy for the periodic purging of Change Audit data.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To set the Change Audit Purge Policy:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Set Purge Policy**.

The Purge Policy dialog box appears in the Periodic Purge Settings pane.

Step 2 Enter the following information:

Field	**Description**
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged. The default is 180 days.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. The default is 180 days. See Tracking RME Server Changes Using Audit Trail for further information.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the purge job for Change Audit and Audit Trail records. To do this, select one of these options from the drop down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule.
at	Enter the start time, in the hh:mm:ss format (23:00:00).
Job Info	
Job Description	The system default job description, *ChangeAudit Records - default purge job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Caution You might delete data by changing these values. If you change the number of days to values lower than the current values, messages over the new limits will be deleted.

Step 3 Click either **Save** to save the purge policy that you have specified, or click **Reset** to reset the changes made to a Purge policy.

Performing a Forced Purge

You can perform a Forced Purge of Change Audit, as required.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To perform a Change Audit Forced Purge:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Force Purge**.

The Purge Policy dialog box appears.

Step 2 Enter the information required to perform a Forced Purge:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. See Tracking RME Server Changes Using Audit Trail for further information.
Scheduling	
Run Type	You can specify when you want to run the force purged job for Change Audit and Audit Trail records. To do this, select one of these options from the drop down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time.
Date	Enter the start date in the dd-mmm-yyyy format, for example, 02-Dec-2003, or click on the Calendar icon and select the date. The Date field is enabled only if you have selected Once as the Run Type.
at	Enter the start time, in the hh:mm:ss format (23:00:00). The At field is enabled only if you have selected Once as the Run Type

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 3 Click **Submit** for the forced purge to become effective.

Config Change Filter

You can use this option to enable or disable VLAN Change audit filtering. When there is a change to the device configuration, a change record is created. By default, the VLAN change audit record is created for those devices that have a VLAN configuration.

To enable or disable the VLAN Change Audit Filter option:

Step 1 Select **Resource Manager Essentials > Admin > Change Audit > Config Change Filter**

The **Config Change Filter** dialog box appears.

Step 2 Check or uncheck the **Enable VLAN Change Audit Filter** option.

- Check **Enable vlan Change Audit Filter**, if you do not want the change audit record to be created for devices that have a VLAN configuration.
- Uncheck **Enable vlan Change Audit Filter**, if you want the change audit record to be created for devices that have VLAN configuration. By default, this option is unchecked.

Step 3 Click either **Apply** to apply the option or click **Cancel** to discard the changes.

Defining Exception Periods

An Exception period is a time you specify when no network changes should occur. This period does not prevent you from making any changes in your network. The set of Exception periods is known as an Exception profile.

You can have only one Exception period for a day.

You perform the following tasks for Exception profiles:

Tasks	Description
Creating an Exception Period	Creating an exception profile.
Enabling and Disabling an Exception Period	Enabling and disabling a set of exception profiles.
Editing an Exception Period	Editing an exception profile.
Deleting an Exception Period	Deleting a set of exception profiles.

Creating an Exception Period

To create an Exception profile:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select:

- Days of the week from the Day drop-down list box
- Start and end times from the Start Time and the End Time drop-down list box.

Step 3 Click **Add**.

The defined exception profile appears in the List of Defined Exception Periods pane.

To enable the exception period, see Enabling and Disabling an Exception Period.

Enabling and Disabling an Exception Period

To enable and disable a set of exceptions periods:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select one or more exception profiles in the List of Defined Exception Periods pane.

Step 3 Click **Enable/Disable**.

- If you have selected Enabled, then the exception period report is generated for that specified time frame.
- If you have selected Disabled, then the exception period report is not generated for that whole day.

For example: If you have disabled exception period for Monday from 10:00 am to 12:30 pm, then there will not be any exception period report generated for Monday.

Editing an Exception Period

To edit an exception profile:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select a day from the Day drop-down list box for which you want to change the exception period.

Step 3 Change the start and end times in the Start Time and the End Time drop-down list box.

If required you can also enable or disable the status for the exception period.

Step 4 Click **Add**.

The edited exception profile appears in the List of Defined Exception Period dialog box. This will overwrite the existing exception profile for that day.

Deleting an Exception Period

To delete a set of Exceptions Periods:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select one or more exception profiles in the List of defined Exception Periods pane.

Step 3 Click **Delete**.

Defining Automated Actions

You can define automated actions on creation of change audit record. This automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are:

- E-mail
- Traps
- Automated scripts

Understanding the Automated Action Window

This window contains the following entries:

Field	Description
Name	Name of the automated action.
Status	Status of the automated action—Enabled, or disabled.
Type	Type of automated action—Email, Script or Trap.

You perform the following tasks from this window:

Tasks	Description
Creating an Automated Action	Creating an automated action.
Enabling and Disabling an Automated Action	Enabling and disabling a set of automated actions. This button gets activated only after selecting an automated action.
Editing an Automated Action	Editing an automated action. This button gets activated only after selecting an automated action.
Exporting and Importing an Automated Action	Exporting and importing a set of automated actions.
Deleting an Automated Action	Deleting a set of automated actions. This button gets activated only after selecting an automated action.

Creating an Automated Action

To create an automated action:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Click **Create**.

The Define Automated Action dialog box appears.

Step 3 Enter the following:

Field	Description
Name	Name for the automated action.
Status	Select either Enabled or Disabled For the automated action to trigger.
Application	Select the name of the application on which the automated action has to be triggered.
Category	Select the types of the changes, for example, configuration, inventory, or software on which the automated action has to be triggered.
Mode	Select the connection mode on connection modes on which the automated action has to be triggered.
User	Select the user name on which the automated action has to be triggered.

Step 4 Click **Next**.

The Automated Action Type dialog box appears.

Step 5 Select either **E-mail** or **Trap** or **Script**. Based on your selection, enter the following data:

If you have selected E-mail, enter...	
Field	**Description**
Send To	Enter the E-mail ID for which the trigger has to be notified. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). You will receive the e-mail with the CiscoWorks E-mail ID as the sender's address.
Subject	Enter the subject of the e-mail.
Content	Enter the content of the e-mail.
If you have selected Trap, perform...	

Enables configuration of a single or dual destination port numbers and hostnames for the traps generated by Change Audit.

Ensure that you have copied these files:

- CISCO-ENCASE-MIB.my
- CISCO-ENCASE-APP-NAME-MIB.my

into the destination system to receive the traps.

These files are available in the following directories on RME server:

On UNIX:

/opt/CSCOpx/objects/share/mibs

On Windows:

NMSROOT\objects\share\mibs. Where *NMSROOT* is the root directory of the CiscoWorks Server.

a. Enter the Server and Port details in the Define Trap field.

b. Click **Add**.

   The server and port information appears in the List of Destinations text box.

   If you want delete, the server and port information, select the server and port information from the List of Destinations text box and click **Delete**.

If you have selected Script, enter...

You can run only shell scripts (*.sh) on Unix and batch files (*.bat) on Windows. The shell script or batch file should have only write/execute permissions for casuser:casusers in solaris and casuser/Administrator in Windows. The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the *casuser* account.

The script files *must* be available at this location:

On UNIX:

/var/adm/CSCOpx/files/scripts/changeaudit

On Windows:

NMSROOT/files/scripts/changeaudit

To select the script file:

a. Click **Browse**.

   The Server Side File Browser dialog box appears with the predefined location.

b. Select the script file (*.sh on Unix and *.bat on Windows)

c. Click **OK**.

Step 6 Click **Finish**.

The Automated Action window appears with the defined automated action.

Editing an Automated Action

To edit an automated action:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Select an Automated Action.

Step 3 Click **Edit**. (See step 3 to step 5 in Creating an Automated Action.).

Step 4 Click **Finish**.

The Automated Action window appears with the updated data.

Enabling and Disabling an Automated Action

To enable or disable a set of automated actions:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Select a or a set of Automated actions.

Step 3 Click **Enable/Disable**.

The Automated Action window appears with the updated data.

Exporting and Importing an Automated Action

To export or import an automated action:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 If you want to export an Automated action, then select the automated actions else go to next step.

Step 3 Click **Export/Import**.

The Export/Import dialog box appears.

Step 4 Select the task to be performed—**Export** or **Import**.

Step 5 Either:

- Enter the filename along with the absolute path.

Or

- Click **Browse**,

  The Server Side File Browser dialog box appears.

a. Select a folder.

b. Click **OK**.

c. Enter the filename.

Step 6 Click **OK**.

Deleting an Automated Action

To delete a set of automated actions:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Select a or a set of Automated actions.

Step 3 Click **Delete**.

The Automated Action window appears with the updated data.

Using Change Audit Reports

You can generate the following reports based on Change Audit data:

- Generating an Exception Period Report
- Generating 24 Hours and Standard Change Audit Reports

You can generate change audit data in XML format using the `cwcli export changeaudit` command line tool This tool also provides servlet access to change audit data.

See Overview: cwcli export Command for generating the Change Audit data in XML format.

You can performing the following actions using these icons on the Change Audit reports:

Button	Description
Export to File (Icon)	You can export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Generating an Exception Period Report

This option lets you compile a report on changes that occurred in the network during a specific time period. This report is based on the Exceptions profiles you set up to occur as often as each day for a week.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate a Exception Period Report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Change Audit** from the first drop-down list box.

Step 3 Select **Exception Period Report** from the second drop-down list box.

Step 4 Select the required devices using the Device Selector. (See Using RME Device Selector for more information.)

Step 5 Enter the information required to generate the required report:

Field	Description
Date Range	
From	Click on the calendar icon and select the start date.
To	Click on the calendar icon and select the end date.
Exception Period	
Select Day(s)	Select the days for the week. If the exception profiles are defined, then the exception periods are displayed in this box. If the exception profiles are not defined, then this box will be blank. You can define your exceptions profiles in the Exception Period Definition dialog box (Resource Manager Essentials > Tools > Change Audit > Exception Periods).
Scheduling	
Run Type	You can specify when you want to run the Exception Report job. To do this, select one of these options from the drop down menu: Immediate—Runs the report immediately. Once—Runs the report once at the specified date and time.

Field	Description
Date	Click on the calendar icon and select the start date. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
at	Select the hours and minutes from the drop-down lists.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. The Job Description field is enabled only if you have selected an option other than Immediate in the Run Type field.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 6 Click **Finish**.

- If you have selected the Run Type as Immediate, then the report appears in a separate browser window.

  If you have selected the Run Type as Once, then a message is displayed:

  ```
  Job ID created successfully.
  Go to Reports->Report Jobs to view the job status.
  ```

  Where *ID* is a unique Job number.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Generating 24 Hours and Standard Change Audit Reports

This option lets you compile a report on all changes that occurred in the network during a specific time period. You can compile a report based on the selection criteria, such as application, users, connection mode.

You can also generate these report using Device Center (from CiscoWorks LMS Portal home page, select Device Troubleshooting > Device Center to launch Device Center).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate the 24 Hour and Standard Reports:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Change Audit** from the first drop-down list box.

Step 3 Select **Standard Report** from the second drop-down list box.

Step 4 Select the required devices using the Device Selector. (See Using RME Device Selector for more information.)

Step 5 Enter the information required to generate the required report:

Field	Description
Date Range	
24 Hours	Select this option, only if you want to generate a 24 hours report. This report will contain all the Change Audit data gathered during the last 24 hours.
From	Click on the calendar icon and select the start date. The From field is enabled only if you have de-selected the 24 Hours check box.
To	Click on the calendar icon and select the end date. The To field is enabled only if you have de-selected the 24 Hours check box.
Selection Criteria	
User Name	Select the user name. This report will be filtered on user names.
Mode	Select the connection mode through which the change was made. This report will be filtered on connection modes.
Category	Select the types of the changes. The supported categories are: • CONFIG_CHANGE—Configuration changes on the device. • INVENTORY_CHANGE—Hardware changes on the device. • SOFTWARE_CHANGE—Software changes on the device.
Application	Select the name of the application. This report will be filtered on application names.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Standard Report job. To do this, select one of these options from the drop down menu: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	Click on the calendar icon and select the start date. The Date field is enabled only if you have selected an option other than Immediate, in the Run Type field.
At	Select the hours and minutes from the drop-down lists.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. The Job Description field is enabled only if you have selected an option other than Immediate, in the Run Type field.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 6 Click **Finish**.

- If you have selected the Run Type as Immediate, then the report appears in a separate browser window.
- If you have selected an option other than Immediate, in the Run Type field, then a message is displayed:

```
Job ID created successfully.
Go to Reports->Report Jobs to view the job status.
```

Where *ID* is a unique Job number.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Understanding Change Audit Report

Change Audit report provides a summary and, when available, detailed record information.

Note When an application is unable to obtain information for Change Audit, N/A is used on the Change Audit report.

The Change Audit report contains all change information provided by RME applications based on your filter criteria. It contains the following fields.

Table 13-1 Change Audit Report

Field	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
User Name	Name of the user who performed the change. This is the name entered when the user logged in. It can be the name under which the RME application is running, or the name using which the change was performed on the device. The User Name field may not always reflect the user name. The User Name is reflected only when: • Config change was performed using RME. • Config change was performed outside of RME, but the network has username based AAA security model, wherein authentication is performed by a AAA server which could be TACACS/RADIUS or local.
Application Name	Name of the RME application involved in the network change. For example, Archive Mgmt, ConfigEditor, CwConfig, etc.
Host Name	Host name of the machine from which the user accessed the device or the host name of the RME server. The Host name can contain IP address if the address does not resolve to a name.
Creation Time	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Connection Mode	Connection mode through which the change was made. For example, Telnet, SNMP, or console. The mode is obtained by querying the device and if the query fails, `default` or `NA` is shown.
Message	Brief summary of the network change.

Table 13-1 Change Audit Report (continued)

Field	Description
Details	Application details for a particular device displayed in a separate browser window. Select the highlighted **Details** text to view application details in a separate browser window. Applications that make or detect changes in the network log a change record in Change Audit log and provide a means for getting to the detailed data. The following information is displayed when you click on the Details link for: • Archive Mgmt, ConfigEditor, CwConfig, and NetConfig—The Config Diff Viewer window is displayed. This window shows the differences between the configurations. See Understanding the Config Diff Viewer Window for further information. • ICServer—The Inventory Change report is displayed. This window shows the changed values (previous and current value) of different Inventory entitites such as FlashDevice, FlashPartition, FlashFile. • Software Management—The Software Modification History report is displayed. This window shows the changed software image details.
Grouped Records	Similar change details grouped by the same job ID and the same function ID (for example: inventory collection) displayed in a separate summary window. Select the highlighted **More Records** text in the Grouped Records column to view similar change details in a frame below the summary window. For example, you have completed a software update on five devices. The Change Audit report shows the Software Management summary information about who performed the job, when, and so on. To display all devices affected by this upgrade, click **More Records** to display the summary information related to the five devices. From here you can look at details of the individual device upgrades.

ChangeAudit Process

The change audit process consists of the following Java programs, which provide the back-end functionality of Device Configuration:

- CasServer
- ConfigArchive
- InvChangeProbe
- Scheduler

This process depends on the following:

- RMEDbMonitor
- CTMJrmServer
- jrm

Stopping and Restarting the Change Audit Process

The following procedure describes the steps to stop and restart the ChangeAudit Process:

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Common Services > Server Configuration > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select the ChangeAudit process.

Step 3 Click either **Stop** to stop the process or **Start** to Restart the process.

CHAPTER 14

Enabling and Tracking Syslogs Using Syslog Analyzer and Collector

The Syslog Analyzer application along with the syslog collector lets you centrally log and track syslog messages (error, exception, information etc) sent by devices in the network. The logged message data can be used to analyze network device performance. Syslog Analyzer application can also be customized to store and produce the information important to you.

The Syslog Analyzer application, or the Syslog Analyzer, works together with the Common Syslog Collector (CSC) (see Overview: Common Syslog Collector).

The Syslog Analyzer receives syslogs from the Common Syslog Collector, invokes automated actions that have been configured for RME, and stores the syslogs in the database. You can use the Syslog Analyzer to generate many useful reports on the syslogs stored in the database. You can also define templates for custom reports.

Network devices can be configured to send Syslog messages directly to the Common Syslog Collector installed on the CiscoWorks Server or a remote network host on which a Syslog Collector is installed. The Common Syslog Collector is configured to filter and forward messages to the CiscoWorks Server.

In addition, Syslog Analyzer application also notifies:

Inventory application, when a network device sends a inventory change syslog messages like SYS-5-RELOAD, SNMP-5-COLDSTART etc. For a complete list of messages that trigger Inventory collection see Table 14-1

Table 14-1 Messages that Trigger Inventory Collection

Facility	Sub-facility	Severity	Mnemonic	Description
*	*	*	RESTART	*
RESTART	*	*	*	*
OIR	*	6	INSCARD	*
SYS	*	5	ONLINE	*
SNMP	*	5	COLDSTART	*
SYS	*	5	RELOAD	*
CPU_REDUN	*	6	BOOTED_AS_ACTIVE	*
CPU_REDUN	*	5	SWITCHOVER	*
Nodemgr	*	5	CE	*REBOOT*

Config Management application, when a network device sends configuration change messages like SYS-6-CFG_CHG, CPU_REDUN-6-RUNNING_CONFIG_CHG etc. For a complete list of messages that trigger a Configuration fetch see Table 14-2.

Table 14-2 Messages that Trigger a Configuration Fetch Operation

Facility	Subfacility	Severity	Mnemonic	Description
*	*	*	RESTART	*
RESTART	*	*	*	*
SYS	*	5	ONLINE	*
*	*	*	CONFIG_I	*
SYS	*	5	RELOAD	*
CONFIG	*	*	*	*
*	*	*	CONFIG	*
OIR	*	6	INSCARD	*
Nodemgr	*	5	CE	*REBOOT*
CPU_REDUN	*	6	BOOTED_AS_ACTIVE	*
CPU_REDUN	*	5	SWITCHOVER	*
CPU_REDUN	*	6	RUNNING_CONFIG_CHG	*
CPU_REDUN	*	5	RCSF_SYNCED	*
CPU_REDUN	*	6	STARTUP_CONFIG_CHG	*
CPU_REDUN	*	5	STARTUP_CONFIG_SYNCED	*
SNMP	*	5	COLDSTART	*
SYS	*	6	CFG_CHG	*telnet*
SYS	*	6	CFG_CHG	*Console*
*	*	*	OIR	*
PIX	*	5	111005	*
SYS	*	6	CFG_CHG	*SNMP*
SYS	*	6	CFG_CHG	*SSH*

Devices send Syslog messages that contain a time stamp reflecting the local time zone of the device. Syslog reports are always displayed in server time zone.

If a device time zone is an unsupported format, the server time zone is used. If a device is not configured to send time zone information with its messages, Syslog assumes that the device resides in the server time zone and uses that time zone in the message time stamp.

For example, assume that a managed device in India (set to the local time zone) sends a Syslog message to an RME server in California. When this message is viewed on a client browser in New York, the message will reflect California time.

Caution Any change that you make to the system time or time zone affects the Syslog processes and other RME processes. You will then have to restart the Daemon Manager for the proper functioning.

Using the Syslog Analyzer application is easy.

After,

- Configuring the network devices,
- Installing a Syslog Collector,
- Registering it with Syslog Analyzer,

you can use Syslog Analyzer to do these tasks:

- View Syslog Collector status for message statistics (see Viewing Common Syslog Collector Status).
- Set the purge policy, to specify the age of a message up to which it should be stored (see Setting the Purge Policy).
  You can also perform a forced purge (see Performing a Forced Purge).
- Set the backup policy (see Setting the Backup Policy).
- Define custom message report templates (see Creating a Custom Report Template).
- Generate standard and custom reports, including 24-hour reports (see Understanding Message Reports).
- Define message filters to exclude or include certain messages from Syslog Analyzer (see Defining Message Filters).
- Define automated actions with which you can add and edit instructions (e-mail, URL or script) to be executed automatically whenever a specific message type is reported (see Defining Automated Actions).

You can generate the following reports and summaries using the Report Generator (**RME > Reports > Report Generator**):

- 24-Hour Report— Generate a report to show data for the past 24 hours. See Generating a Standard Report.
- Syslog Custom Summary Report—Shows a summary of all custom reports. This is created and added by the system administrator.
  See Generating a Syslog Custom Summary Report.
- Severity Level Summary Report—Summarizes messages in order of severity level (emergencies, alerts, critical, etc.). You can select a group of devices and a range of dates for your report. From this summary, you can display detailed reports of each type of message.
  See Generating a Severity Level Summary Report.
- Standard Report—Shows logged messages for a group of devices within a selected range of dates.
  See Generating a Standard Report.
- Unexpected Device Report—Provides syslog information from all the devices on your network, that have not been added to RME, if they have been configured to send messages to the server.
  See Generating an Unexpected Device Report.

You can also define custom reports templates using the Custom Reports Templates option (**RME > Reports > Custom Reports Templates**). The reports templates that you create are displayed in the Report Generator.

Note You can select the log level settings for the Syslog application using the feature Application Log Level Settings (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

For the new features in this release, see What's New in this Release.

Overview: Common Syslog Collector

Common Syslog Collector is a service to receive, filter and forward syslogs to one or more Syslog Servers, thus reducing traffic on the network as well as processing load on the server.

The Common Syslog Collector can be installed on the CiscoWorks Server, or on a remote UNIX or Windows machine, to process Syslog messages. You can uninstall the Syslog Collector later if you no longer want to run it on a remote UNIX or Windows server.

Common Syslog Collector (CSC) is a service that runs independently, listens for syslogs and forwards them to the registered applications after necessary filtering. This way, the parsing/filtering is taken away from the applications and each device sends only one copy of the processed, valid syslogs to the Common Syslog Collector. Even though CSC runs independently, it can run either remotely or locally on the machine where an application is running.

The RME server and the Syslog Collector exchange updates such as status, and filters.

You can configure the service to read syslogs from a specified file. This can be provided in a properties file located at:

On Solaris:

NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/
Collector.properties

On Windows:

NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\
Collector.properties

See the *Installation and Setup Guide for Resource Manager Essentials*, for the complete details.

In a scenario where the devices and the CSC may run in two different time zones, the syslogs will be marked with timestamp of the CSC if they do not have a timestamp when they are received, or if the format is not correct.

The device considers day-light-saving settings appropriately while putting the timestamps. CSC supports all the time zones that Common Services 3.0 supports, and alternatively you can provide the time zone information. See the *Installation and Setup Guide for Resource Manager Essentials*, for the complete details.

After the Syslog Analyzer has been registered with the Collector, it:

- Receives the filters it needs from the RME server to filter Syslog messages.
- Sends status to the Syslog Analyzer process about the collected Syslog messages upon request from the Analyzer, including the number of messages read, number of messages filtered, and number of messages with bad syntax. It also forwards unfiltered messages to the Syslog Analyzer process.

  If the Syslog Analyzer does not send any filters, then the Collector sends all the syslogs to the Analyzer without filtering.

If the RME server is restarted, Syslog Collector will lose communication to the RME server. Based on the current filters, it continues to filter the syslogs and stores them in a local file:

NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\server name_port\DowntimeSyslogs.log

The Syslog Analyzer will automatically restore the connection after RME server restart.

For the complete instructions on installing the Common Syslog Collector, see the Installation and Setup Guide for Resource Manager Essentials.

Viewing Status and Subscribing to a Common Syslog Collector

Using the Syslog Collector Status dialog box you can:

- View the status of your Common Syslog Collector (see Viewing Common Syslog Collector Status).
- Subscribe to a Common Syslog Collector (see Subscribing to a Common Syslog Collector).

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Viewing Common Syslog Collector Status

To view the status of the Common Syslog Collector to which the Syslog Analyzer is subscribed to, follow this procedure:

Select **Resource Manager Essentials > Tools > Syslog > Syslog Collector Status**.

The Collector Status dialog box appears, with this information:

Column	Description
Name	Hostname or the IP address of the host on which the Collector is installed.
Forwarded	Number of forwarded Syslog messages
Invalid	Number of invalid Syslog messages.
Filtered	Number of filtered messages. Filters are defined with the option Message Filters option (see Defining Message Filters.)
Dropped	Number of Syslog messages dropped.
Received	Number of Syslog messages received.
Up Time	Time duration for which the Syslog Collector has been up.
Update Time	Date and time of the last update. Time and time zone are those of the CiscoWorks Server.

If you want to refresh the information in this dialog box, click **Update**.

If you have restarted the RME daemon manager, the Syslog Collector Status processes (under **Resource Manager Essentials > Tools > Syslog**) may take 6-10 minutes to come up, after the Syslog Analyze processes come up. In this interval you may see the following message:

```
Collector Status is currently not available.
Check if the SyslogAnalyzer process is running normally.
```

Wait for the Syslog Collector status process to come up and try again.

To subscribe to a Common Syslog Collector using the Subscribe button, see Subscribing to a Common Syslog Collector.

Subscribing to a Common Syslog Collector

Before you subscribe to a Common Syslog Collector, ensure these pre-requisites are met:

Check whether:

1. The Self-signed Certificates are valid. For example, check for the expiry date of the certificates on both the servers.
2. The Self-signed Certificates from this server are copied to the Syslog Collector server and vice-versa.

   To do this, go to **Common Service Administration > Server Configuration > Security**. Use the Peer certificate dialog box. See the User Guide for Common Services for more details.
3. The SyslogCollector process on Syslog Collector server and SyslogAnalyzer process on this server, are restarted after Step 2.
4. Both hosts are reachable by host name.

To subscribe to a Common Syslog Collector:

Step 1 Select **Resource Manager Essentials > Tools > Syslog**.

The Collector Status dialog box appears. For the information in the columns in the dialog box, see Viewing Common Syslog Collector Status:

Step 2 Click **Subscribe**.

The following message appears:

```
Check if:

Self-signed Certificates from this server are copied to the Syslog Collector server and
vice-versa. You can perform this operation from Common Service Administration > Server
Configuration > Security > Peer certificate screen.

2. Syslog Collector process on SyslogCollector server and SyslogAnalyzer process on this
server is restarted after step 1.

3. Both hosts are reachable by host name.

4. Certificates are valid.

The Subscribe Collector dialog box appears.
```

Step 3 Click **OK**.

Step 4 Enter the address of the Common Syslog Collector to which you want to subscribe to.

Step 5 Click **OK**.

The Syslog Analyzer server is subscribed to the specified Common Syslog Collector.

If you are already subscribed to a Syslog collector, and you want to unsubscribe, select the collector and click the Unsubscribe button.

Understanding the Syslog Collector Properties File

After installing the Syslog Collector on a remote system, you need to check the Syslog Collector Properties file to ensure that the Collector is configured properly.

The Syslog Collector Properties file is available at this location:

On Solaris:

$NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties

On Windows:

%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties

The following table describes the Syslog Collector Properties file:

Timezone-Related Properties	**Description**
TIMEZONE	The timezone of the system where the Syslog Collector is running. Enter the correct abbreviation for the timezone. For example, the time zone for India is IST. For the correct Timezone abbreviation, see the Timezone file in the following location: On Solaris, /opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst On Windows, *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\TimeZone.lst See Timezone List Used By Syslog Collector.
COUNTRY_CODE	Country code for the Syslog Collector. We recommend that you set the country code variable with the appropriate country code, to make sure that the Syslog timestamp conversion works correctly. For example, if you are in Singapore, you must set the country code variable as **COUNTRY=SGP**.

Timezone-Related Properties	Description
TIMEZONE_FILE	The path of the Timezone file. This file contains the offsets for the time zones. After installing the Syslog Collector, ensure that the offset specified in this file is as expected. If it is not present or is incorrect, you can add the Timezone offset as per the convention. The default path is: On Solaris, opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst On Windows, *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\TimeZone.lst
General Properties	
SYSLOG_FILES	Filename and location of the file from which syslog messages are read. The default location is: On Solaris: /var/log/syslog_info On Windows: *%NMSROOT%*\log\syslog.log
DEBUG_CATEGORY_NAME	Name Syslog Collector uses for printed ERROR or DEBUG messages. The default category name is SyslogCollector. We recommend that you do not change the default value.
DEBUG_FILE	Filename and location of the Syslog Collector log file containing debug information: The default location is: On Solaris, /var/adm/CSCOpx/log/CollectorDebug.log On Windows, *%NMSROOT%*\log\CollectorDebug.log
DEBUG_LEVEL	Debug levels in which you run the Syslog Collector. We recommend that you retain the default INFO, which reports informational messages. Setting it to any other value might result in a large number of debug messages being reported. If you change the debug level, you must restart the Syslog Collector. The values for the Debug levels are: • Warning • Debug • Error • Info

Timezone-Related Properties	**Description**
DEBUG_MAX_FILE_SIZE	The maximum size of the log file containing the debug information. The default is set to 5 MB. If the file size exceeds the limit that you have set, Syslog Collector writes to another file, based on the number of backup files that you have specified for the DEBUG_MAX_BACKUPS property. For example, if you have specified the number of backups as 2, besides the current log file, there will be two backup files, each 5MB in size. When the current file exceeds the 5 MBlimit, Syslog Collector overwrites the oldest of the two backup files.
DEBUG_MAX_BACKUPS	The number of backup files that you require. The size of these will be the value that you have specified for the DEBUG_MAX_FILE_SIZE property.
Miscellaneous Properties	
READ_INTERVAL_IN_SECS	The interval at which the Collector polls the syslog file. The default is set to 1 second.
QUEUE_CAPACITY	The size of the internal buffer, for queuing syslog messages. The default is set to 100000
PARSER_FILE	The file that contains the list of parsers used while parsing syslog messages. The default path of the parser file: On Solaris, opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/FormatParsers.lst On Windows, *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\FormatParsers.lst
SUBSCRIPTION_DATA_FILE	The Syslog Collector data file that contains the information about the Syslog Analyzers that are subscribed to the Collector. The default path of the data file: On Solaris, opt/CSCOpx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Subscribers.dat On Windows, *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Subscribers.dat
FILTER_THREADS	The number of threads that operate at a time for filtering syslog messages. The default is set to 1.
COLLECTOR_PORT	The default port of the Syslog Collector. The default is set to 4444. The port where the collector listens for registration requests from Syslog Analyzers.

Timezone List Used By Syslog Collector

The timezone of the system where the Syslog Collector is running. In the Syslog Collector Properties file, you must enter the correct abbreviation for the timezone. See Understanding the Syslog Collector Properties File.

For the correct Timezone abbreviation, see the Timezone file in the following location:

$*NMSROOT*/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst

Each entry in the TimeZone.lst file represents a timezone abbreviation, and its offset from GMT. Each offset here is 10 multiplied by the actual offset. For example, the actual offset for IST is 5.5 hours, and the corresponding entry here is 55.

You must use the same method while modifying it.

The following is the timezone list used by SyslogCollector:

Time Zone List Used by Syslog Collector

ACT=95	ADT=30	AET=100	AEST=100	AGT=-30
AHST=-100	ART=20	AST=-90	AT=-20	BET=-30
BST=10	BT=30	CAT=10	CCT=80	CDT=-50
CEST=20	CET=10	CNT=-35	CST=-60	CTT=80
EADT=-110	EAST=100	EAT=30	ECT=10	EDT=-40
EET=20	EST=-50	FST=-20	FWT=10	GMT=0
GST=100	HDT=90	HST=-100	IDLE=120	IDLW=-120
IET=-50	IST=55	JST=90	MDT=-60	MEST=-20
MESZ=-20	MET=10	MEWT=10	MIT=-110	MST=-70
MYT=80	NET=40	NST=120	NT=-110	NZDT=130
NZST=120	NZT=120	PDT=-70	PLT=50	PNT=-70
PRT=-40	PST=-80	SST=110	SWT=10	UTC=0
VST=70	WADT=-80	WAST=70	WAT=-10	YDT=-80
YST=-90	ZP4=40	ZP5=50	ZP6=50	

Using Syslog Analyzer

The following is the workflow for Syslog Analyzer:

Step 1 Configure devices (see Configuring Devices to Send Syslogs).

Step 2 Configure the Common Syslog Collector which is installed during the RME installation, or install another Remote Syslog Collector on another machine (see the Installation and Setup Guide for Resource Manager Essentials).

Step 3 Perform various tasks such as defining and managing filters, automated actions, setting back-up policy, setting the purge policy, performing a forced purge, defining custom reports templates, specifying the path for the Syslog message file, etc.

See:

- Setting the Backup Policy
- Setting the Purge Policy
- Performing a Forced Purge
- Defining Custom Report Templates
- Defining Custom Report Templates
- Defining Automated Actions
- Defining Message Filters

Step 4 Generate various reports such as Custom Summary report, Severity Level Summary report, Standard Report, Unexpected Device report and Workflow report. See:

- Overview: Syslog Analyzer Reports
- Generating a Syslog Custom Summary Report
- Generating a Severity Level Summary Report
- Generating a Standard Report
- Generating an Unexpected Device Report

Using Syslog Service on Windows

System message logging is not part of the Windows operating system. Therefore, the CiscoWorks Server provides logging service to Windows users.

The logging service saves each system message to *NMSROOT*\log\syslog.log (where *NMSROOT* is the RME installation directory).

Syslog Analyzer reads and processes the messages in this file, and writes them to the RME database. The Syslog processes use the database information to generate Syslog reports.

When the syslog.log file gets too big, you can stop the Syslog Analyzer (**Start > Settings > Control Panel > Services**) and delete the log file.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select **SyslogCollector** and click **Stop**.

Step 3 Open the Windows Control Panel and select **Administrative tools > Services**.

Step 4 Select **CWCS syslog service**, and click **Stop**.

Step 5 Delete the *NMSROOT*\log\syslog.log file.

- To restart the syslog service in the Control Panel, click **Start** next to the **CWCS syslog service**.

- To restart the SyslogAnalyzer process in RME, select **Common Services > Server > Admin > Processes** and click **Start**.

Checking the Syslog Configuration File on UNIX

Check the path and permissions of the file pointed to by local7.info in the syslog configuration file /etc/syslog.conf on the RME server.

Note The first occurrence of local7 in the syslog.conf file, must contain the path for the Syslog message source.

Step 1 Make sure that the facility.level definition is set to local7.info, and that the following line is present (there must be a tab between local7.info and the path/filename):

```
local7. info path/filename
```

Step 2 Make sure that the syslog process (syslogd) can both read and write to the file.

- If you modify the /etc/syslog.conf file, you must restart the syslog process (syslogd). Enter the following command to stop and restart syslogd:

  ```
  /etc/init.d/syslog stop
  /etc/init.d/syslog start
  ```

- If the start and stop command do not work, enter:

  ```
  kill -HUP 'cat /etc/syslog.pid'
  ```

Step 3 Make sure the path for Syslog message file in the CiscoWorks Server is the same as the filename you specified in the syslog.conf file.

Stopping and Restarting Syslog Analyzer

To stop Syslog Analyzer:

Step 1 Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select **SyslogAnalyzer**.

Step 3 Click **Stop**.

To restart Syslog Analyzer:

Step 1 Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select **SyslogAnalyzer**.

Step 3 Click **Start**.

Viewing Syslog Analyzer Status

You can check Syslog status using this option.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Click **Common Services > Server > Admin > Processes.**

The Process Management dialog box appears.

Step 2 Click **SyslogAnalyzer** (hyperlink) to view process details.

The Process Details window appears.

Field	Data
Process	Process name
Path	Fully qualified path name for the Java Runtime Environment (JRE)
Flags	Java package name and class file of the Syslog Analyzer program
Startup	When the process was started
Dependencies	Prerequisite processes

Configuring Devices to Send Syslogs

Syslog Analyzer lets you centrally log and track system error messages, exceptions, and other information (such as device configuration changes) that you can use to analyze device and network performance.

Configure devices to forward messages to the RME server or to a system on which you have installed the Common Syslog Collector. For details about the Syslog Collector, see the Installation Guide for RME 4.0.

For more information about setting up devices for message logging, see the Cisco IOS Software Documentation on Cisco.com.

On UNIX systems, make sure that the Syslog facility for the device is set to local7. Messages from devices are continuously added to the file pointed to by the logging facility local7.info in the /etc/syslog.conf (syslog configuration) file.

The first occurrence of local7 in the syslog.conf file, must contain the path for the Syslog message source.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

You can configure the devices for sending Syslog messages to RME server in the following ways:

- Configuring the Device Using Telnet
  - IOS Devices
  - Catalyst Devices
  - Content Service Switches Devices
  - Content Engine Devices
- Configuring the Device Using NetConfig Syslog Task

Configuring the Device Using Telnet

This section details how to configure devices using Telnet.

IOS Devices

To configure IOS devices using Telnet:

Step 1 Connect to the device using Telnet and log in.

The prompt changes to host>.

Step 2 Enter **`enable`** and the enable password.

The prompt changes to host#.

Step 3 Enter **`configure terminal`**.

You are now in configuration mode, and the prompt changes to host(config)#.

- To make sure logging is enabled, enter **`logging on.`**
- To specify the RME server to receive the router Syslog messages, enter **`logging`** *IP address*, where *IP address* is the server IP address.
- To limit the types of messages that can be logged to the RME server, enter **`logging trap informational`** to set the appropriate logging trap level by, where informational signifies severity level 6. This means all messages from level 0-5 (from emergencies to notifications) will be logged to the RME server.

Step 4 Verify that the syslog filter settings are correct and that syslog is running.

Catalyst Devices

To configure Catalyst devices using Telnet:

Step 1 Connect to the device using Telnet and log in.

The prompt changes to `host`.

Step 2 Enter **`enable`** and the enable password.

The prompt changes to `host#`.

- To make sure logging is enabled, enter **`set logging server enable`**.
- To specify the RME server that is to receive the Catalyst devices Syslog messages, enter **`set logging server`** *IP address*, where IP address is the server IP address.
- To limit the types of messages that can be logged to the RME server, enter **`set logging level all 6 default`**. This means that all messages from level 0-5 (from emergencies to notifications) will be logged to the RME server.

Step 3 See the appropriate Catalyst reference manual for more information.

Step 4 Verify that the syslog filter settings (see Defining Message Filters) are correct and that syslog is running.

Content Service Switches Devices

To configure Content Service Switches (CSS) devices using Telnet:

Step 1 Connect to the device using Telnet and enter into the Global Configuration mode.

Step 2 Run the following commands:

logging commands enable

`logging host` *CiscoWorks IP address*

logging facility local7

Content Engine Devices

To configure Content Engine (CE) devices using Telnet:

Step 1 Connect to the device using Telnet and enter into the Global Configuration mode.

Step 2 Run the following commands:

`logging host` *CiscoWorks IP address*

logging facility local7

NAM Devices

To configure NAM devices using Telnet:

Step 1 Connect to the device using Telnet and enter into the Global Configuration mode.

Step 2 Run the following commands:

`remote-host` *CiscoWorks IP address*

logging facility local7

PIX Devices

To configure PIX devices using Telnet:

Step 1 Connect to the device using Telnet and enter into the Global Configuration mode.

Step 2 Run the following commands:

`logging host` *CiscoWorks IP address* [*in_if_name*] *CiscoWorks IP address* [*protocol /port*] [**`format emblem`**], where:

in_if_name is the interface on which the syslog server resides.

CiscoWorks IP address is the address of the CiscoWorks server.

protocol is the protocol over which the syslog message is sent; either tcp or udp. PIX Firewall only sends TCP syslog messages to the PIX Firewall Syslog Server.

You can only view the port and protocol values you previously entered by using the write terminal command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17.

port is the port from which the PIX Firewall sends either UDP or TCP syslog messages. This must be same port at which the syslog server listens.

For the UDP port, the default is 514 and the allowable range for changing the value is 1025 through 65535.

For the TCP port, the default is 1470, and the allowable range is 1025 through 65535. TCP ports only work with the PIX Firewall Syslog Server.

`format emblem` is the option that enables EMBLEM format logging on a per-syslog-server basis. EMBLEM format logging is available for UDP syslog messages only and is disabled by default.

Configuring the Device Using NetConfig Syslog Task

This section details how to configure devices using the NetConfig Syslog task.

Use the job definition wizard in NetConfig to create and schedule a NetConfig job. For more details see the Making and Deploying Configuration Changes Using NetConfig topics.

See the following procedure to launch the NetConfig application and use the NetConfig Syslog task in a job:

Step 1 Select **Resource Manager Essentials > Config Mgmt > NetConfig**.

The NetConfig Job Browser appears.

Ensure that you have set the transport protocol order and password policy for your job using **Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt**. See the topics Configuring Transport Protocols and Configuring Default Job Policies in the section, Archiving Configurations and Managing Them Using Archive Management.

For the fields in the NetConfig Job Browser, see Starting a New NetConfig Job in the section Making and Deploying Configuration Changes Using NetConfig.

Step 2 Click **Create**.

The Devices and Tasks dialog box appears, with these panes:

Table 14-3 Panes in the Devices and Tasks Dialog Box

Pane	Description
Device Selector	Allows you to select the devices on which the NetConfig job has to run. Make sure that for the devices on which the job will run, the configurations are archived in the Configuration Archive. NetConfig will not configure devices whose configurations are not archived. (See Archiving Configurations and Managing Them Using Archive Managementon how to update the configuration archive.)
Task Selector	Allows you to select the system-defined tasks or user-defined tasks that you want to run on the selected devices. For descriptions of system-defined tasks and the device categories they support, seeCreating and Editing User-defined Tasks in the section Making and Deploying Configuration Changes Using NetConfig.

Step 3 Select the devices from the Device Selector pane.

For details about the Device Selector, see the topic Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management.

Step 4 Select the required task from the All tab, Using the Task Selector.

Your selection appears in the Selection pane. You can select one or more task at a time.

Step 5 Click **Next.**

The Add Tasks dialog box appears with these panes:

Table 14-4 Panes in the Add Tasks Dialog Box

Pane	Description
Applicable Tasks	Allows you to add a task. The task that you selected using the Task Selector, appears here. From your selection, only the tasks that are applicable to at least one device that you have selected, appear here. If the task that you have selected does not apply to the categories of any of the devices that you have selected, it will not be displayed in the Applicable Tasks pane. Select a task and click **Add** to create an instance for the task (see Step 6).
Added Instances	Allows you to edit the task instance you have added, view its CLI, or delete it. Select the instance of the task, and click the required button (see Table 9-1).

Table 14-5 Tasks Performed by Buttons in the Added Instances Pane

Button	Description
Edit	Task pop-up opens with previously assigned values. You can edit these values and click **Save**.
View CLI	Device Commands pop-up opens with the list of applicable devices and their corresponding CLI commands. Devices in your selection for which the commands are not applicable, are also displayed as Non-Applicable Devices. Click **Close**. You can edit an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.
Delete	Deletes the selected task instance. You can delete an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.

Step 6 Select the Syslog configuration task from the Applicable Tasks pane and click **Add**.

The Syslog Configuration Task (system-defined or user-defined) pop-up appears for the selected task (seeCreating and Editing User-defined Tasks in the section Making and Deploying Configuration Changes Using NetConfig).

This is a dynamic user interface. The Syslog Configuration task dialog box displays parameters based on your device selection in the Device Selector. For example, if you have selected Content Engine devices, you will be able to specify Content Engine parameters in this dialog box. If not, this section will not be available to you.

Step 7 Set the parameters in the task dialog box and click **Save**.

(To reset the values that you have selected click **Reset**. Click **Cancel** to return to the previous dialog box, without saving your changes.)

You will see the instance of the task in the Added Tasks pane of the Add Tasks dialog box. The instance appears in this format:

Taskname_n, where *Taskname* is the name of the task you have added, and *n* is the number of the instance. For example, the first instance of a Banner task is `Banner_1`.

You can add as many instances as required, for a task.

Step 8 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 9 Set the schedule for the job, in the Scheduling pane.

Step 10 Set the job options, in the Job Options pane.

To view the device order, click **Device Order**. The Set Device Order pop-up appears.

You can reset the order in which the job should be executed on the devices using the up and down arrows. When you are done, click **Done**. The pop-up closes.

Step 11 Click **Next**.

The Job Work Order dialog box appears with the general information about the job, the job policies, the Job Approval details (if you have enabled job approval), the device details, the task, and the CLI commands that will be executed on the selected devices as part of this job.

Step 12 Click **Finish** after you review the details of your job in the Job Work Order dialog box.

A job confirmation message appears along with the Job ID. The newly created job appears in the NetConfig Job Browser.

For the complete procedure on how to schedule the NetConfig job see Starting a New NetConfig Job in the section Making and Deploying Configuration Changes Using NetConfig.

Also see Syslog Task in the section Making and Deploying Configuration Changes Using NetConfig.

Syslog Administrative Tasks

You can perform the following Administrative tasks:

- Back up syslog messages (see Setting the Backup Policy).
- Purge syslog messages (see Setting the Purge Policy).
- Perform a forced purge (see Performing a Forced Purge).

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform these tasks.

Setting the Backup Policy

The Backup Configuration feature allows you to save the Syslog messages to a flat file. The syslog data that is trimmed from the database will be moved to the flat file.

Note In Solaris, the backup file is created with `-rw-r----- casuser casusers` irrespective of the permissions given to the directory for backup on purge. In Windows, the backup file inherits the permission and ownership of the directory it is created in, which is the directory selected as the backup location (on purge).

View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To set up the backup policy:

Step 1 Select **Resource Manager Essentials > Admin > Syslog > Set Backup Policy**.

The Backup Policy dialog box appears.

By default, the backup policy is set to disabled.

Step 2 Select **Enable** to enable the backup process for Syslog messages, after configuring backup.

Step 3 Click **Browse** to select the backup file location.

The Server Side File Browser dialog box appears.

In the Server Side File Browser dialog box:

a. Specify the external file.

b. Select Directory Content,

c. Click **OK**.

Step 4 Enter the maximum size that you want to set for the backup file. By default this is set to 100 MB.

Step 5 Enter the e-mail ID of the user who should receive a notification, if the backup fails. You can enter multiple e-mail addresses separated with commas. This is a mandatory field.

Configure the SMTP server to send e-mails in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**).

We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.)

If you also want a notification to be sent when the backup is a success, select **Also Notify on Success**.

Step 6 Either click **Save** to save the backup configuration details that you have specified or click **Reset** to clear the values that you specified and reset to the previously saved values in the dialog box.

If you have clicked Save, the backup will continue to save the data even after the data has exceeded the specified size of the backup file. However, the system will send an e-mail asking you to cleanup the backup file.

Setting the Purge Policy

You can specify a default policy for the periodic purging of Syslog messages.

If you access a table either through immediate reports, report jobs or by any other means, the database locks the table and therefore the table will not be successfully purged. However, during the successive purge operations such a table will be purged.

A purge job is enabled by default, and is scheduled to run at 1:00 AM daily.

To specify your default purge policy:

Step 1 Select **Resource Manager Essentials > Admin > Syslog > Set Purge Policy**.

The Purge Policy dialog box appears.

Step 2 Specify the number of days in the **Purge records older than** field.

Only the records older than the number of days that you specify here, will be purged. The default value is 7 days. This is a mandatory field.

Caution You might delete data by changing these values. If you change the number of days to values lower than the current values, messages over the new limits will be deleted.

If the data of a particular day is being accessed either through immediate reports, report jobs, or by any other means, it will not be purged. However, during the successive purge operations this data will be purged.

Step 3 Specify the periodicity of the purge in the Run Type field. This can be monthly, daily, or weekly.

Step 4 Select the start date using the calendar icon, to populate the date field in the dd-mmm-yyyy format (For example, 02-Dec-2004). This is a mandatory field.

Step 5 Enter the start time in the At field, in the hh:mm:ss format (23:00:00). This is a mandatory field.

The Job Description field has a default description—`Syslog Records - default purge job`.

Enter the e-mail ID of the user who should be notified when the scheduled purge is complete. You can enter more than one e-mail ID separated by commas. This is a mandatory field. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**).

We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address

Step 6 Either click **Save** to save the purge policy that you have specified or Click **Reset**. to clear the values that you specified and reset the defaults in the dialog box.

You can view the scheduled purge job in the Common Services JRM Job Browse (**Common Services > Server > Admin > Job Browser**).

Performing a Forced Purge

You can perform a forced purge of Syslog messages, as required.

If you access a table either through immediate reports, report jobs or by any other means, the database locks the table and therefore the table will not be successfully purged. However, during the successive purge operations such a table will be purged.

To perform a forced purge:

Step 1 Select **Resource Manager Essentials > Admin > Syslog > Force Purge**.

The Force Purge dialog box appears.

Step 2 Enter the information required to perform a Forced Purge:

Field	Description
Purge records older than	Enter the number of days. Only the records older than the number of days that you specify here, will be purged. This is a mandatory field. If the data of a particular day is being accessed either through immediate reports, report jobs, or by any other means, it will not be purged. However, during the successive purge operations this data will be purged.
Scheduling	
Run Type	Specify whether the purge is to be immediate or once. • If you select Immediate, all the other options will be disabled for you. • If you select Once, you can specify the start date and time and also provide the job description (mandatory) and the e-mail ID for the notification after the scheduled purge is complete. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.
Date	Select the start date using the calendar icon, to populate the Date field in the dd-mmm-yyyy format, for example, 02-Dec-2004. This is a mandatory field. The Date field is enabled only if you have selected Once as the Run Type.
at	Enter the start time, in the hh:mm:ss format (23:00:00). The at field is enabled only if you have selected Once as the Run Type.
Job Info	

Field	Description
Job Description	Enter a description for the forced purge job. The Job Description field is enabled only if you have selected Once as the Run Type. This is a mandatory field. Accepts alphanumeric values.
E-mail	Enter the e-mail ID of the user who should be notified when the Forced Purge is complete. You can enter more than one e-mail ID separated by commas. The e-mail field is enabled only if you have selected Once as the Run Type. Configure the SMTP server to send e-mails in the View/ Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address

Step 3 Click **Submit** for the Forced Purge to become effective.

To clear the values that you specified and reset the defaults in the dialog box, Click **Reset**.

You can view the scheduled force purge job in the Common Services JRM Job Browse (**Common Services > Server > Admin > Job Browser**).

Defining Custom Report Templates

When you create a custom report template, you select the syslog message types you want reported. The Custom Templates option lets you create a custom template, and edit or delete existing custom templates.

When you select **Resource Manager Essentials > Reports > Custom Templates**, a list of all Custom Templates is displayed in the dialog box on the Custom Templates page.

The columns in the Custom Templates dialog box are:

Column	Description
Template Name	Name of the template.
Report Type	Syslog report, or inventory report.
Owner	The user who created the template.
Last Modified Time	The date (yyyy-mm-dd) and the time (hh:mm:ss).

Using the custom templates dialog box, you can do the following tasks:

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Task	**Button**
Create a custom template (see Creating a Custom Report Template).	Create
Editing a custom template (see Editing a Custom Template).	Edit
Delete a custom template (see Deleting a Custom Template).	Delete

Creating a Custom Report Template

To create a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates.**

The custom templates dialog box appears.

Step 2 Click **Create**.

The Application Selection dialog box appears.

Step 3 Select **Syslog**.

Step 4 Click **Next**.

The Syslog custom report template dialog box appears. The messages that have previously been defined are displayed here.

The columns in the Syslog custom reports templates dialog box are:

Column	**Description**
Facility	Facility is a hardware device, a protocol, or a module of the system software; for example, SYS. See the Cisco IOS reference manual System Error Messages for a predefined list of facility codes.
Sub-Facility	Sub-Facility is the subfacility in the device that generated the Syslog message. In most cases, this is blank. An example of an entry in this field is CCM_CDR_INSERT-GENERIC-0-OutOfMemory.
Severity	The severity level for the messages. The following are the severity codes: 0—Emergencies 1—Alerts 2—Critical 3—Errors 4—Warnings 5—Notifications 6—Informational
Mnemonic	Code that uniquely identifies the error message. For example, UPLOAD, RELOAD,CONFIG.
Description	Description of the Syslog message.

Step 5 Enter a unique name for the custom report template, in the Custom Report Name field.

Step 6 Specify whether you want the custom report template to be Public or Private.

Public templates can be seen and used by other users who have the permissions to do these tasks. Private templates can be seen and used by only owner (creator) of the templates.

Using the Syslog custom report template dialog box, you can do the following tasks:

Task	Button
Add a message type (see Adding a Message Type.)	Use the Add button.
Edit a message type (see Editing a Message Type.)	Use the Edit button.
Delete a message type (see Deleting a Message Type.)	Use the Delete button.
Select a message type from a set of standard messages (see Selecting a Message Type.)	Use the Select button.

Step 7 Click **Finish**.

A confirmation message appears that the report has been successfully created.

Your custom report template is displayed in the dialog box on the Custom Templates page (**Resource Manager Essentials > Reports > Custom Templates**).

To run the report, see Running a Custom Report.

Adding a Message Type

To add a message type:

Step 1 Click **Add** in the Define New Message Type section of your dialog box.

The Define New Message Type dialog box appears.

Step 2 Enter the required information:

Column	Description
Facility	Enter the codes for the facilities you want reported. A facility is a hardware device, a protocol, or a module of the system software. See the Cisco IOS reference manual, System Error Messages, for a predefined list of system facility codes. Each code can consist of two or more uppercase letters. You can enter several facility codes, separated by commas, for example, SYS,ENV,LINK. If you do not enter any facility but use the asterisk, all the facilities will be reported.
Sub-Facility	Enter the codes for the sub-facilities you want reported. Sub-Facility is the subfacility in the device that generated the Syslog message. An example of an entry in this field is CCM_CDR_INSERT-GENERIC-0-OutOfMemory. This is an optional field. If you do not enter any sub-facility but use the asterisk, all the sub- facilities will be reported.

Column	Description
Severity	Enter codes for the message severity levels you want reported. The following codes are supported: 0—Emergencies 1—Alerts 2—Critical 3—Errors 4—Warnings 5—Notifications 6—Informational If you do not enter any severity level but use the asterisk, all severity levels will be considered.
Mnemonic	Enter a code that uniquely identifies the error message. To match for Catalyst 5000 family devices, enter a hyphen (-) to indicate an empty mnemonic field. You can enter several mnemonics, separated by commas. An example is UPLOAD, RELOAD,CONFIG.
Description	Enter the Syslog message description. For example, *REBOOT*, *SNMP*, *telnet*, etc. If you do not want to specify a description, leave in the default asterisk.

Step 3 Click **Save**.

The new message type is added, and appears in the Define New Message Type section of your dialog box.

If you want to save the information and add another message type, click **Save and Add**.

Deleting a Message Type

To delete a message type:

Step 1 Select the required message type from the Define New Message Type section of your dialog box.

Step 2 Click **Delete**.

You will be asked to confirm the deletion. If you confirm the deletion, the message type is deleted.

Editing a Message Type

To edit a message type:

Step 1 Select the required message type from the Define New Message Type section of your dialog box

Step 2 Click **Edit**.

The Define New Message Type dialog box appears with the previously entered information in the fields (for the field descriptions, see Adding a Message Type).

Step 3 Edit the information and click **Save**.

The message type is edited.

Selecting a Message Type

To select a system defined message type:

Step 1 Click **Select** in the Define New Message Type section of your dialog box.

The Select System Defined Message Types dialog box appears.

Step 2 Select the required system defined message type.

Step 3 Click **OK**.

The selected message appears in the Define New Message Type section of your dialog box.

Editing a Custom Template

To edit a custom template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The custom templates dialog box appears with a list of custom templates.

Step 2 Select the required custom template and click **Edit**.

Step 3 The Syslog custom report template dialog box appears. The messages that have previously been defined, appear here.

For the description of the columns in the Syslog custom reports templates dialog box, see Creating a Custom Report Template.

If required, you can:

- Change the Custom Report accessibility—Private to Public or vice-versa.
- Add a message type (see Adding a Message Type.)
- Edit a message type (see Editing a Message Type.)
- Delete a message type (see Deleting a Message Type.)
- Select a message type from system-defined message types (see Selecting a Message Type.)

Step 4 Click **Finish**.

The edited custom template appears in the custom templates dialog box.

Deleting a Custom Template

To delete a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The custom templates dialog box appears with a list of custom templates.

Step 2 Select the required custom template.

Step 3 Click **Delete**.

You will be asked to confirm the deletion. If you confirm the deletion, the template will be deleted.

The Syslog custom report template is deleted and no longer appears in the Syslog custom report template dialog box.

Running a Custom Report

You can run any custom report that you previously created. Custom report templates that you created, appear in the Report Generator drop-down list box for Syslog, with a separator.

To create a custom report template, see Defining Custom Report Templates.

To run a Syslog custom report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, select Syslog.

Step 3 Go to the second drop-down list box, select the required custom report. (Custom reports that you created appear in the drop-down list box with a separator).

The Device Selector appears, along with the fields that allow you to enter information in the Scheduling and Job Info fields.

Step 4 Select the required devices using the Device Selector. (See the topic, Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management, for more details.)

Step 5 Enter the information required to generate the required custom report, in the Date Range, Scheduling, and Job Info groups:

Field	Description
Date Range	
24 Hours	Select this option, only if you want to generate a 24 hour report. This report will contain all the syslog data gathered during the last 24 hours. For example, if you select this option and schedule the report to be generated at 6.p.m. the report will have the data of the past 24 hours, from 6 p.m.
From	Click on the calendar icon and select the date. The date appears in the dd-mmm-yyyy format in the From field. For example, 02-Dec-2004. The From field is enabled only if you have de-selected the 24 Hours check box.
To	Click on the calendar icon and select the date. The date appears in the dd-mmm-yyyy format in the To field. For example, 03-Dec-2004. The To field is enabled only if you have de-selected the 24 Hours check box.

Field	Description
Scheduling	
Run Type	Specifies the type of schedule for the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly— Runs monthly on the day of the month and at the specified time. In the case of periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. If you select Immediate, the Date, Job Description, and E-mail option will be disabled for you. If you select any other run type, then you can specify the start date and time and also provide the job description (mandatory) and the e-mail ID for the notification after the report is generated.
Date	Select the start date using the calendar icon, to populate the Date field in the dd-mmm-yyyy format, for example, 02-Dec-2004. This is a mandatory field. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
at	Select the time in hours and minutes from the respective drop-down lists.

Field	Description
Job Info	
Job Description	Enter a description for the report that you are creating. The Job Description field is enabled only if you have selected an option other than Immediate in the Run Type field. This is a mandatory field. Accepts alpahnumeric characters.
E-mail	Enter the e-mail ID of the user who should be notified when the report is generated. You can enter more than one e-mail ID, separated by commas. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address

Step 6 Click **Finish**.

If you had selected the Run Type as Immediate, the report appears immediately in a separate browser window. If you had selected a Run Type other than Immediate, this confirmation message appears:

```
Job <Job ID> created successfully.
Go to Reports->Report Jobs to view the job status.
```

Where *Job ID* is the unique ID of the job.

To view Report Jobs, go to **Resource Manager Essentials > Reports->Report Jobs**. For details see the topic Using the Reports Job Browserin the section Generating Reports.

Defining Automated Actions

You can create automated actions to be executed automatically whenever Syslog Analyzer receives a specific message type.

When you select **Resource Manager Essentials > Tools > Syslog > Automated Actions**, a list of automated actions appears in the dialog box on the Automated Actions page. Of these, there are two system-defined automated actions (the rest are user-defined). The system-defined automated actions are:

- Inventory Fetch—To fetch inventory from the device.
- Config Fetch—To fetch configuration from the device.

You can edit these system-defined automated actions, but you cannot delete them. These actions are enabled by default. You can choose to disable them by selecting them and clicking **Enable/Disable**.

Config Fetch might loop if SYS-6-CFG_CHG-*SNMP* message is received from a Catalyst operating system device. You can then edit Config Fetch automated action and you can delete SYS-6-CFG_CHG-*SNMP* message type. For more details, see Deleting a Message Type.

In the Automated Actions dialog box, you can choose whether to include interfaces of selected devices or not.

The columns in the Automated Actions dialog box are:

Column	Description
Name	Name of the automated action.
Status	Status of the automated action at creation time—Enabled, or disabled
Type	Type of automated action—E-mail, script or URL.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Using the automated actions dialog box, you can do the following tasks:

Task	Button
Create an automated action (see Creating an Automated Action).	Create
Edit an automated action (see `Editing an Automated Action).	Edit
Enable or Disable an automated action (see Enabling or Disabling an Automated Action)	Enable/Disable
Import or Export an automated action (see Exporting or Importing an Automated Action)	Import/Export
Delete an automated action (see Deleting an Automated Action).	Delete

If you are creating an automated action, see the example (Automated Action: An Example) of how to set up an automated action that sends an e-mail when a specific Syslog message is received.

On Windows, you cannot set up an automated action to execute an.exe file that interacts with the Windows desktop. For example, you cannot make a window pop up on the desktop.

Creating an Automated Action

To create an automated action:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, with a list of automated actions, appears in the Automated Actions page. Here, you can choose whether to include interfaces of selected devices or not. For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Click **Create**.

A dialog box appears for device selection.

Step 3 Select **All Managed Devices** or **Choose Devices**.

If you select the All Managed Devices option:

- You cannot select the individual devices or device categories from the device selector.
- All managed devices are considered.
- The syslog messages from the various device interfaces are considered for creating automated actions.

If you select Choose Devices option, you must select the required devices (for details about the Device Selector, see the topic Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management).

Step 4 Click **Next**.

A dialog box appears in the Define Message Type page.

Step 5 Enter a unique name for the automated action that you are creating.

Step 6 Select either **Enabled** or **Disabled** as the status for the action at creation time.

Step 7 Select the Syslog message types for which you want to trigger the automated action from the Define New Message Type section of the dialog box. (For explanations of the column titles Facility, Sub-facility, Severity etc., see Adding a Message Type.)

If you want to add, delete, edit, or selected system-defined Syslog message types, see:

- Adding a Message Type,
- Selecting a Message Type
- Editing a Message Type
- Deleting a Message Type

Step 8 Click **Next**.

The Automated Action Type dialog box appears.

Step 9 Select a type of action (E-mail, URL, or Script) from the Select a type of action drop-down list box.

- If you select E-mail, enter the following information in the Automated Action Type dialog box:

Field	Description
Send to	List of comma separated e-mail addresses. Mandatory field.
Subject	Subject of the e-mail.
Content	Content that you want the e-mail to contain.

- If you select URL, enter the URL to be invoked, in the URL to Invoke field of the Automated Action type dialog box. In the URL, you can use the following parameters:
  - $*D* (for the device)
  - $*M* (for the complete syslog message).

  When the URL is invoked, If you have specified $*D* or $*M*, then, $*D* is substituted with the device hostname or IP address and $*M* is substituted with the syslog message.

  For example, if the URL is

  http://*hostname/script.pl?device=$D&mesg=$M*

  When invoked, $*D* is replaced with 10.68.12.2 and $*M* is replaced with the URL-encoded syslog message.

- If you select Script, enter the script to be used, in the Script to execute field of the Automated Action type dialog box.

  Either enter or select the script file. You can run only shell scripts (*.sh) on Unix and batch files (*.bat) on Windows. The shell script or batch file should have only write/execute permissions for casuser:casusers in UNIX and casuser/Administrator in Windows.

The other users should have only read permission. You must ensure that the scripts contained in the file have permissions to execute from within the casuser account.

The script files must be available at this location:

On Windows:

NMSROOT/files/scripts/syslog

On UNIX:

/var/adm/CSCOpx/files/scripts/syslog

To select the script file:

- Click **Browse**.

  The Server Side File Browser dialog box appears.
- Select the file (*.sh on Unix and *.bat on Windows).

Step 10 Click **OK**.

Step 11 Click **Finish**.

If the executable program produces any errors or writes to the console, the errors will be logged as Info messages in the SyslogAnalyzer.log.

This file is available at:

On UNIX,

/opt/CSCOpx/log directory

On Windows,

NMSROOT\log directory (where *NMSROOT* is the root directory of the CiscoWorks Server).

`Editing an Automated Action

To edit an automated action:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, displaying the list of automated actions, appears in the Automated Actions page.

For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Select an automated action from the drop-down list and click **Edit**.

The Select Devices dialog box appears.

Step 3 Select the required devices and click **Next**.

A dialog box appears in the Define Message Type page.

This dialog box allows you to:

- Change the Message Filter Type—From Enabled to Disabled, or vice, versa.
- Add a message type (see Adding a Message Type.)
- Edit a message type (see Editing a Message Type.)

- Delete a message type (see Deleting a Message Type.)
- Select a message type from system-defined message types (see Selecting a Message Type.)

Step 4 Click **Next**.

Step 5 The Automated Action Type dialog box appears.

This dialog box allows you to change the type of action. For example, you can change from E-mail to URL or Script.

- For E-mail, enter or change the following information in the Automated Action type dialog box:

Field	Description
Send to	The list of comma separated e-mail addresses.
Subject	The subject of the e-mail (optional).
Content	The content that you want the e-mail to contain.

Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**).

We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address

- For URL, enter or change the URL to be invoked, in the Automated Action type dialog box. If you select URL, enter the URL to be invoked, in the URL to Invoke field of the Automated Action type dialog box. In the URL, you can use the following parameters:
  - $*D* (for the device)
  - $*M* (for the complete syslog message).

  When the URL is invoked, If you have specified $*D* or $*M*, then, $*D* is substituted with the device hostname or IP address and $*M* is substituted with the syslog message.

  For example, if the URL is

  http://*hostname/script.pl?device=$D&mesg=$M*

  When invoked, $*D* is replaced with 10.68.12.2 and $*M* is replaced with the URL-encoded syslog message.

- If you select Script, enter the script to be used, in the Script to execute field of the Automated Action type dialog box.

  Either enter or select the script file. You can run only shell scripts (*.sh) on Unix and batch files (*.bat) on Windows. The shell script or batch file should have only write/execute permissions for casuser:casusers in UNIX and casuser/Administrator in Windows.

  The other users should have only read permission. You must ensure that the scripts contained in the file have permissions to execute from within the casuser account.

  The script files must be available at this location:

  On Windows:

  NMSROOT/files/scripts/syslog

  On UNIX:

  /var/adm/CSCOpx/files/scripts/syslog

- To select the script file, click **Browse**.

  The External Config Selector dialog box appears.
- Select the file (*.sh on Unix and *.bat on Windows).

Step 6 Click **Finish**.

The edited automated action appears in the dialog box on the Automated Action page.

Guidelines for Writing Automated Script

To write an automated script:

Step 1 Copy the sampleEmailScript.pl from RME 3.5 or older to the new RME 4.1 server and put this file in:

For Solaris:

/var/adm/CSCOpx/files/scripts/syslog directory

For Windows:

NSMROOT/files/scripts/syslog

Step 2 Write a shell script for Solaris or .bat file for Windows in the same directory.

Here is an example shell script (called syslog-email.sh) for UNIX:

```
#!/bin/sh

/opt/CSCOpx/bin/perl /var/adm/CSCOpx/files/scripts/syslog/sampleEmailScript.pl
-text_message "MEssage:

$2 from device: $1" -email_ids nobody@nowhere.com -subject "Syslog Message: $2" -from
nobody@nowhere.com -smtp mail-server-name.nowhere.com
```

For Windows, replace $1 and $2 with %1 and %2 and change the directory accordingly.

Enabling or Disabling an Automated Action

To enable or disable an automated action:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, displaying the list of automated actions, appears in the Automated Action page.

For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Select the required automated action from the list in the dialog box.

Step 3 Click **Enable/Disable** to toggle its status.

The dialog box in the Automated Action page is refreshed and it displays the changed state for the specified automated action.

Exporting or Importing an Automated Action

You can export an automated action to a flat file and use this file on any Syslog Analyzer, using the import option.

To export or import an automated action:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, displaying the list of automated actions, appears in the Automated Action page.

For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Select an automated action. You can select more than one automated action.

If you do not select an automated action before clicking the Export/Import button, then only the Import option will be available. The Export option will be disabled

Step 3 Click **Export/Import**.

The Export/Import Automated Actions dialog box appears with the Export or Import options.

Step 4 Select either **Export** or **Import**.

Step 5 Either:

- Enter the location of the file to be exported or imported.

Or

- Click **Browse**.

  The Server Side File Browser appears. You can select a valid file, and click **OK**.

The file location appears in the Export/Import dialog box.

Step 6 Click **OK**.

Deleting an Automated Action

To delete an automated action:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, displaying the list of automated actions, appears in the Automated Action page.

For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Select the required automated action from the list in the dialog box.

Step 3 Click **Delete**.

You will be asked to confirm the deletion. If you confirm the deletion, the action will be deleted.

Automated Action: An Example

This is an example of how to set up an automated action that sends an e-mail when a specific Syslog message is received. This example assumes that devices have been imported and are sending Syslog messages to the CiscoWorks server.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Automated Actions**.

A dialog box, with a list of automated actions, appears in the Automated Action page. For the description of the columns in the Automated Actions dialog box, see Defining Automated Actions.

Step 2 Click **Create**.

The Devices Selection dialog box appears.

Step 3 Select the required devices and click **Next**.

The Define Message Type dialog box appears.

Step 4 Enter a unique name for the automated action that you are creating.

Step 5 Select either **Enabled**, or **Disabled** as the status for the action at creation time.

Step 6 Click **Select**.

The Select System Defined Message Types dialog box appears.

Step 7 Select the SYS folder, then select the SYS-*-5-CONFIG_I message from the Select System Defined Message Types list, and click **OK**.

The dialog box on the Define Message Type page appears.

Step 8 Click **Next**.

The Automated Action Type dialog box appears.

Step 9 Select the type of action—E-mail, Script, or URL.

If you had selected Email in Step 9: Enter the following information:

Field	Description
Send to	List of comma-separated e-mail addresses.
Subject	Subject of the e-mail (optional).
Content	Content that you want the e-mail to contain.

Configure the SMTP server to send e-mails in the View/Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**).

We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). If a syslog is found with the matching type for managed (normal) devices, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address. Then go to Step 10.

If you had selected Script in Step 9: Choose the appropriate bat file for Windows, or shell script for Solaris, from the File Selector. For details about these files, see the topic Creating an Automated Action. Then go to Step 10.

If you had selected URL in Step 9: Enter the URL to be invoked. If you select URL, enter the URL to be invoked, in the URL to Invoke field of the Automated Action type dialog box. In the URL, you can use the following parameters:

- $*D* (for the device)
- $*M* (for the complete syslog message).

When the URL is invoked, if you have specified $*D* or $*M*, then, $*D* is substituted with the device hostname or IP address and $*M* is substituted with the syslog message.

For example, if the URL is

http://*hostname/script.pl?device=$D&mesg=$M*

When invoked, $*D* is replaced with *10.68.12.2* (where *10.68.12.2* is the IP address of the device) and $*M* is replaced with the URL-encoded syslog message.

Step 10 Click **Finish**.

Also see Verifying the Automated Action.

Verifying the Automated Action

To verify the automated action:

Step 1 Select a managed router that is already sending Syslog messages to the RME server and generate a SYS-5-CONFIG_I message by changing the message-of-the-day banner as follows:

- **a.** Connect to the managed router using Telnet and log in.
- **b.** In enable mode enter **`enable`**, then enter a password.
- **c.** At the config prompt enter **`configure terminal`**.
- **d.** Change the banner by entering:

```
banner motd z
This is a test banner z
end
```

- **e.** Exit the Telnet session.

Step 2 Make sure that the SYS-5_CONFIG_I message is sent to the CiscoWorks Server as follows:

- On UNIX systems, open the syslog_info file located in the /var/log directory, or whichever file has been configured to receive Syslog messages.
- On Windows systems, open the syslog.log file located in the *NMSROOT*\log\ directory.

  Where *NMSROOT* is the RME installation directory.

Step 3 Verify that there is a message from the managed router whose banner-of-the-day was changed.

This message appears at the bottom of the log.

- If the message is in the file, an e-mail is mailed to the e-mail ID specified.

- If the message is not in the file, the router has not been configured properly to send Syslog messages to the CiscoWorks Server.

Defining Message Filters

You can exclude messages from Syslog Analyzer by creating filters.

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To launch the message filters dialog box:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters.**

A dialog box appears in the Message Filters page.

A list of all message filters is displayed in this dialog box, along with the names, and the status of each filter—Enabled, or Disabled.

Step 2 Specify whether the filters are for dropping the Syslog messages or for keeping them, by selecting either **Drop** or **Keep**.

- If you select **Drop**, the Common Syslog Collector drops the syslogs that match any of the Drop filters from further processing.
- If you select **Keep**, Collector allows only the syslogs that match any of the “Keep” filters, for further processing.

Note The Drop or Keep options apply to all message filters. They do not apply to individual filters.

Step 3 Specify whether interfaces of selected devices should be included.

In the dialog box that displays the message filters, you can do the following tasks:

Task	Button
Create a filter (see Creating a Filter).	Create
Edit a filter (see Editing a Filter).	Edit
Enable or disable a filter (see Enabling or Disabling a Filter).	Enable/Disable
Export or import a filter. (see Exporting or Importing a Filter).	Export/Import
Delete a filter (see Deleting a Filter).	Delete

Creating a Filter

You can create a filter for Syslog messages by:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A dialog box with a list of filters, appears in the Message Filter page.

Step 2 Specify whether the filter should be a dropped or kept, by selecting either **Drop** or **Keep**.

- If you select **Drop**, the Common Syslog Collector drops the Syslogs that match any of the “Drop” filters from further processing.
- If you select **Keep**, Collector allows only the Syslogs that match any of the “Keep” filters, for further processing.

Note The Drop or Keep options apply to all message filters. They do not apply to individual filters.

Step 3 Click **Create**.

The dialog box appears for device selection. Select All Managed Devices or Choose Devices.

If you select All Managed Devices option:

- You cannot select the individual devices or device categories from the device selector.
- All managed devices are considered.
- The syslog messages from the various device interfaces are considered for creating message filters.

If you select the Choose Devices option, you must select the required devices (for details about the Device Selector, see the topic Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management).

Step 4 Click **Next**.

.A dialog box appears in the Define Message Type page.

Step 5 Enter a unique name for the filter.

Step 6 Select either the Enabled, or the Disabled status for the filter at creation time.

Step 7 Select the Syslog message types for which you want to apply the filter.

If you want to add, delete, edit, or select system-defined Syslog message types, see:

- Adding a Message Type
- Selecting a Message Type
- Editing a Message Type
- Deleting a Message Type

Step 8 Click **Finish**.

The list of filters in the message filter dialog box on the Message Filters page is refreshed.

Editing a Filter

To edit a filter:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A dialog box, displaying the list of filters, appears in the Message Filter page.

Step 2 Select a filter by clicking on its check box, and click **Edit**.

The Select Devices dialog box appears.

Step 3 Select the required devices and click **Next**.

A dialog box appears in the Define Message Type page.

This dialog box allows you to:

- Change the filter Status—From Enabled to Disabled, or vice versa.
- Add a message type (see Adding a Message Type.)
- Edit a message type (see Editing a Message Type.)
- Delete a message type (see Deleting a Message Type.)
- Select a message type from system-defined message types (see Selecting a Message Type.)

Step 4 Click **Finish** after you make all your changes.

The edited filter appears in the dialog box on the Message Filter page.

Enabling or Disabling a Filter

To enable or disable a filter:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A dialog box, with the list of filters, appears in the Message Filter page.

Step 2 Select the required filter from the list in the dialog box.

Step 3 Click **Enable/Disable** to toggle its status.

The dialog box in the Message Filter page is refreshed and it displays the changed state for the specified filter.

Exporting or Importing a Filter

You can export a filter to a flat file and use this file on any Syslog Analyzer, using the import option.

To export or import a filter:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A dialog box, with the list of filters, appears in the Message Filter page.

Step 2 Select a filter. You can select more than one filter.

Step 3 Click **Export/Import**.

The Export/Import dialog box appears with the Export or Import options.

Step 4 Select either **Export** or **Import**.

Step 5 Either:

- Enter the location of the file to be exported or imported.

Or

- Click **Browse**.

  The Server Side File Browser appears.

  You can select a valid file location, and click **OK**.

  The file location appears in the Export/Import dialog box.

Step 6 Click **OK**.

Deleting a Filter

To delete a filter:

Step 1 Select **Resource Manager Essentials > Tools > Syslog > Message Filters**.

A dialog box, displaying the list of filters, appears in the Message Filter page.

Step 2 Select the required filter from the list in the dialog box.

Step 3 Click **Delete**.

When you confirm the deletion, the filter is deleted.

Overview: Syslog Analyzer Reports

You can use the Syslog Analyze reports to examine your default and custom reports, or to determine the cause of device error messages.

Using the Report Generator of RME, you can generate various Syslog reports:

- Generating a Syslog Custom Summary Report
- Generating a Severity Level Summary Report
- Generating a Standard Report
- Generating an Unexpected Device Report

You can generate 24-hour reports that will show data for the past 24 hours, from the schedule time of the report.

Successfully generated reports are stored in the Archives. You can access the reports archives by selecting **Resource Manager Essentials >Reports > Report Archives** (see the topic Viewing Archived Reports in the section Viewing Archived Reports).

In the Reports Archive/Report jobs, you cannot see the Immediate reports.

If you have selected the Run Type as Immediate, then the report appears in a separate browser window.

If you have selected an option other than Immediate, in the Run Type field, then a message is displayed,

```
Job ID created successfully.
Go to Reports > Report Jobs to view the job status.
```

Here, Job ID is a unique Job number.

An Immediate job displays the first 10,000 lines of a report. For the full report, schedule a job.

Note When you are generating a syslog report, you may get an `outofmemory` exception. This may occur if the number of syslog messages that were generated in the Date Range that you specified in the syslog report job, exceeded six hundred thousand. Specify a shorter Date Range in the Report Generator, and run the report job again.

To use the Report Generator:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Report Generator dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, select Syslog.

Step 3 Go to the second drop-down list box, select the required report, for example, Custom Summary Report.

Step 4 Select the required devices using the Device Selector.

For details about the Device Selector, see the topic Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management.

Step 5 Enter the information required to generate the required report:

Field	Description
Date Range	
24 Hours	Select this option, only if you want to generate a 24 hour report. This report will contain all the syslog data gathered during the last 24 hours. For example, if you select this option and schedule the report to be generated at 6.p.m. the report will have the data of the past 24 hours, from 6 p.m.
From	Click on the calendar icon and select the date. The date appears in the dd-mmm-yyyy format in the From field. For example, 02-Dec-2004. The From field is enabled only if you have de-selected the 24 Hours check box.
To	Click on the calendar icon and select the date. The date appears in the dd-mmm-yyyy format in the To field. For example, 03-Dec-2004. The To field is enabled only if you have de-selected the 24 Hours check box.
Scheduling	

Field	Description
Run Type	Specifies the type of schedule for the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly— Runs monthly on the day of the month and at the specified time. In the case of periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. If you select Immediate, the Date, Job Description, and E-mail option will be disabled for you. If you select any other run type, then you can specify the start date and time and also provide the job description (mandatory) and the e-mail ID for the notification after the report is generated.
Date	Select the start date using the calendar icon, to populate the Date field in the dd-mmm-yyyy format, for example, 02-Dec-2004. This is a mandatory field. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
at	Select the hours and minutes from the drop-down lists.

Field	Description
Job Info	
Job Description	Enter a description for the report that you are creating. The Job Description field is enabled only if you have selected an option other than Immediate in the Run Type field. This is a mandatory field. Accepts alpahnumeric characters.
E-mail	Enter the e-mail ID of the user who should be notified when the report is generated. You can enter more than one e-mail ID, separated by commas. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (**Common Services > Server > Admin > System Preferences**). When the job completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address

Step 6 Click **Finish**.

The specified report appears in a separate browser window.

You can generate the following reports:

- 24-Hour Report. See Generating a 24-Hour Report
- Syslog Custom Report. See Generating a Syslog Custom Summary Report.
- Severity Level Summary Report. See Generating a Severity Level Summary Report.
- Standard Report. See Generating a Standard Report.
- Unexpected Device Report. See Generating an Unexpected Device Report.

If you want to revert to the default values in the RME Reports dialog box, click **Reset**

Understanding Message Reports

All message reports display:

- Timestamp: The date and time the message was logged. This is the timestamp provided by the device. Syslog Analyzer will provide a timestamp if the device does not send one.
- Device name: The name of the router or switch for which the message was logged.
- Facility-Severity-Mnemonic:
  - Facility is a hardware device, a protocol, or a module of the system software, for example, SYS. See the Cisco IOS reference manual, *System Error Messages,* for a predefined list of system facility codes.
  - Severity is the message severity level, from informational (6) to emergency (0).
  - Mnemonic is a code that uniquely identifies the error message. Note that Catalyst 5000 messages do not display a mnemonic. An example of a mnemonic for an IOS message is CONFIG I.

- Subfacility is the subfacility in the device that generated the Syslog message. In most cases this is blank.

  An example of an entry in the Facility-Severity-Mnemonic field is SYS-5-CONFIG I.
- Description is a description of the message.

Each message report also lets you access additional information.

Generating a 24-Hour Report

To generate the report, see Overview: Syslog Analyzer Reports.

Fields in the 24-Hour Report are the same as in the Standard Report. See Generating a Standard Report.

Generating a Syslog Custom Summary Report

The Custom Report Summary Reports option lets you display a list of all custom syslog reports. All syslog reports display message log information.

To generate the report, see Overview: Syslog Analyzer Reports.

Fields in the Custom Summary Report:

Field	Description
Custom Report Name	Name of the Custom Reports.
Total number of records	Number of records that have been generated for each report.

Generating a Severity Level Summary Report

The Severity Level Summary report shows how many emergencies, alerts, critical, errors, warnings, notifications, and informational messages each device has logged.

To generate the report, see Overview: Syslog Analyzer Reports. The fields in the Severity Level Summary Report are given below:

Field	Description
Device Name	Name of the device from which syslog messages are received.
Emergencies	Number of emergency messages received from the device.
Alerts	Number of alert messages received from the device.
Critical	Number of critical messages received from the device.
Errors	Number of error messages received from the device.
Warnings	Number of warning messages received from the device.
Notifications	Number of notification messages received from the device.

Field	Description
Informational	Number of informational messages received from the device.
Debugging	Number of debug messages received from the device.

You can click on any of the field titles to sort the report based on that field.

Generating a Standard Report

You can generate a system message report for a device or set of devices. You can run a report for a date or range of dates and base the report on the message severity or alert types. All Syslog reports display message log information.

Note When you are generating a Standard Report, you may get an `outofmemory` exception. This may occur if the number of syslog messages that were generated in the date range that you specified in the report job, exceeded six hundred thousand. Decrease the period, that is, specify a shorter date range, and run the report job again.

To generate the report, see Overview: Syslog Analyzer Reports.

Fields in the Standard Report:

Field	Description	Link
Device Name	Name of a device (switch or router) that caused the Syslog message.	None.
Interface	The IP address of the interface through which the syslog was sent out.	None.
Timestamp	Date and time the message was logged. This is the timestamp provided by the device. Syslog Analyzer provides a timestamp if the device does not send one.	None.
Facility-SubFacility	• Facility is a hardware device, a protocol, or a module of the system software; for example, SYS. Refer to the Cisco IOS reference manual System Error Messages for a predefined list of facility codes. • SubFacility is the subfacility in the device that generated the Syslog message. In most cases, this is blank. An example of an entry in this field is SYS-5-CONFIG I.	None.
Severity	Message severity level, from informational (6) to emergency (0).	None.
Mnemonic	Code that uniquely identifies the error message. Note that older Catalyst messages do not display a mnemonic. An example of a mnemonic for an IOS message is CONFIG I.	None.

Field	Description	Link
Description	Syslog Message description.	None.
Details	Name of the Syslog message. Displays a new window containing the Syslog message description. When you click on the User_URL icon, you link to a customized web page, if you have defined one; otherwise, it defaults to a sample Perl script for creating a user URL.	This column contains a hyperlinked asterix ('*'). When you click the '*', the description of the Syslog message is displayed.

Generating an Unexpected Device Report

You can generate a report of syslog information for all unmanaged devices on your network. All syslog reports display message log information.

Before you can manage a device, you must add a device to RME (see the topic Adding Devices to RME in the section Adding and Troubleshooting Devices Using Device Management. After the device is added, however, Syslog messages received before adding the device, remain in this report because the Syslog Analyzer does not modify message status.

To generate the report, see Overview: Syslog Analyzer Reports.

The fields in the Unexpected Device Report are:

Field	Description	Link
Device Name	Name/IP of a device (switch or router) that caused the Syslog message.	None.
Time	Date and time the message was logged. This is the timestamp provided by the device. Syslog Analyzer provides a timestamp if the device does not send one.	None.
Facility-SubFacility	• Facility is a hardware device, a protocol, or a module of the system software; for example, SYS. Refer to the Cisco IOS reference manual System Error Messages for a predefined list of facility codes. • SubFacility is the subfacility in the device that generated the Syslog message. In most cases, this is blank. An example of an entry in this field is SYS-5-CONFIG I.	None.
Severity	Message severity level, from informational (6) to emergency (0).	None.
Mnemonic	Code that uniquely identifies the error message. Note that older Catalyst messages do not display a mnemonic. An example of a mnemonic for an IOS message is CONFIG I.	None.
Description	Syslog Message description.	None.
Details	Name of the Syslog message. Displays a new window containing the Syslog message description. When you click on the User_URL icon, you link to a customized web page, if you have defined one; otherwise, it defaults to a sample Perl script for creating a user URL.	This column contains a hyperlinked asterix ('*'). When you click the '*', the description of the Syslog message is displayed.

Using Device Center

The CiscoWorks Common Services Device Center provides a "device-centric" view for CiscoWorks applications and offers you device-centric features and information from one single location.

From the CiscoWorks LMS Portal home page, select **Device Troubleshooting > Device Center**. The Device Center window appears with the device selector on the right and Device Center overview information on the left section of the screen.

Enter the IP address or device name of the device you want to select and click **Go** in the Device Selector field or select a device from the list-tree. The Device Summary and Functions Available panes appear in the right section of the screen.

Click any of the links under the **Functions Available** pane to launch the corresponding application function. The links are launched in a separate window.

Note If you enter the device name or IP address of a device not managed by any of the applications installed on the Common Services server, the Functions Available pane will display only the default connectivity tools from Common Services.

For Syslog application, you can generate the Syslog Analyzer Standard Report.

In the Functions Available pane, select **Reports > Syslog Messages**. The Syslog Analyzer Standard Report appears. For details of this report, see Generating a Standard Report.

Creating a Custom Report: Example

As the network administrator of a network with OSPF (open shortest path first), you know an OSPF-2-NOMEMORY syslog message could potentially result in routing problems. You want to create a custom syslog report that lists OSPF NOMEMORY errors, so that you can run the report and check for problems.

Prerequisites

In this scenario, you will use only the Syslog Analyzer application.

No prerequisites are required.

For a complete description of the required tasks, see the Online Help.

Procedures

The purpose of this scenario is to show you how you can use specific RME applications to perform these tasks. This will help you understand how to use the applications to perform similar tasks in your network.

When you create a custom report template, you select the syslog message types you want reported. The Custom Templates option lets you create a custom template, and edit or delete existing custom templates.

To create a custom report template:

Step 1 Select **Resource Manager Essentials > Reports > Custom Report Templates**.

The custom templates dialog box appears.

Step 2 Click **Create**.

The Application Selection dialog box appears.

Step 3 Select Syslog.

Step 4 Click **Next**.

The Syslog custom report template dialog box appears. The messages that have previously been defined are displayed here.

Step 5 Enter a unique name for the custom report template, in the Custom Report Name field, for example, OSPFNOMEMORY.

Step 6 Specify whether you want the custom report template to be Public or Private.

Public templates can be seen and used by other users who have the permissions to do these tasks. Private templates can be seen and used by only owner (creator) of the templates.

Step 7 Click **Add** in the Define New Message Type section of your dialog box.

The Define New Message Type dialog box appears.

Step 8 Enter the required information:

Column	Description
Facility	You can enter the codes for the facilities you want reported. A facility is a hardware device, a protocol, or a module of the system software. See the Cisco IOS reference manual, System Error Messages, for a predefined list of system facility codes. Each code can consist of two or more uppercase letters. You can enter several facility codes, separated by commas. If you do not enter any facility but use the asterisk, all the facilities will be reported. In this example, enter OSPF.
Sub-Facility	You can enter the codes for the sub-facilities you want reported. Sub-Facility is the subfacility in the device that generated the Syslog message. This is an optional field. If you do not enter any sub-facility but use the asterisk, all the sub- facilities will be reported. In this example, leave in the default asterisk.

Column	Description
Severity	You can enter codes for the message severity levels you want reported. The following codes are supported: 0—Emergencies 1—Alerts 2—Critical 3—Errors 4—Warnings 5—Notifications 6—Informational If you do not enter any severity level but use the asterisk, all severity levels will be considered. In this example, enter 2.
Mnemonic	You can enter a code that uniquely identifies the error message. To match for Catalyst 5000 family devices, enter a hyphen (-) to indicate an empty mnemonic field. You can enter several mnemonics, separated by commas. In this example, enter NOMEMORY
Description	You can enter an appropriate description for the Syslog message. In this example, leave in the default asterisk.

Step 9 Click **Save**.

The new message type is added, and appears in the Define New Message Type section of your dialog box.

If you want to save the information and add another message type, click **Save and Add**.

Step 10 Click **Finish**.

A confirmation message appears that the report has been successfully created.

For more details about the columns in the Syslog custom report template dialog box, see the topic Creating a Custom Report Template in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector.

For more details about the field descriptions of the Define New Message Type dialog box, see the topic, Adding a Message Type in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector.

Verification

To make sure the report was created, select **Resource Manager Essentials > Reports > Custom Templates**.

Your custom report template is displayed in the dialog box on the Custom Templates page.

To run this Syslog custom report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, select Syslog.

Step 3 Go to the second drop-down list box, select the required custom report. (Custom reports that you created appear in the drop-down list box with a separator, therefore your report, OSPFNOMEMORY appears here.)

The Device Selector appears, along with the fields that allow you to enter information in the Scheduling and Job Info fields.

Step 4 Select the required devices using the Device Selector. (See the topic, Using RME Device Selector in the section Adding and Troubleshooting Devices Using Device Management, for more details.)

Step 5 Select 24 Hours in the Date Range group.

Step 6 Select Immediate from the Run Type drop-down list, in the Scheduling group.

Step 7 Click **Finish**.

Your OSPFNOMEMORY custom report appears in a separate browser window.

For more details on Syslog Custom Reports, see the topic Defining Custom Report Templates in the section Enabling and Tracking Syslogs Using Syslog Analyzer and Collector.

CHAPTER 15

Tracking RME Server Changes Using Audit Trail

Audit Trail tracks and reports changes that the RME administrator makes on the RME server.

To view the list of RME tasks that trigger an Audit Trail record, see Audit Trail Record.

You can perform the following tasks using the Audit Trail records:

- Generate a Audit Trail report

  You can track the changes that are performed on the RME server by the RME administrator.

  See Generating a Standard Audit Trail Report for procedure on generating Audit Trail report.

- Purging the Audit Trail records

  Frees disk space and maintains your Audit Trail records at a manageable size. You can either schedule for periodic purge or perform a forced purge of Audit Trail data.

  See Performing Maintenance Tasks for scheduling a periodic purge.

Audit Trail Record

The following RME tasks trigger an Audit Trail record:

Application Name	Tasks	Navigation
Install/Migration	The following Audit records are logged at the time of migration: • Device information is migrated • Syslog message filters are migrated • Syslog automated actions are migrated • Enabling the shadow directory	Not applicable
Change Audit	Setting the Purge Policy. An Audit Trail record is logged any time you make a change in the Purge Policy dialog box.	Resource Manager Essentials > Admin > Change Audit > Set Purge Policy

Application Name	Tasks	Navigation
Change Audit	Performing a Forced Purge. An Audit Trail record is logged when a Force Purge job is scheduled.	Resource Manager Essentials > Admin > Change Audit > Force Purge
Change Audit	An Audit Trail record is logged when you: • Add an automated action. • Enable or disable the automated actions. • Edit an automated action. • Import the automated actions. • Delete the automated actions.	Resource Manager Essentials > Tools > Change Audit > Automated Actions
Change Audit	An Audit Trail record is logged when you: • Add an Exception Profile • Delete the Exception Profiles • Enable or disable the Exception Profiles	Resource Manager Essentials > Tools > Change Audit > Exception Periods
Configuration Management—Archive Management	An Audit Trail record is logged when you: • Change the Archive location • Enable or disable the Shadow directory option	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt
Configuration Management—Archive Management	An Audit Trail record is logged when you: • Enable or disable the Periodic Polling option • Change the Periodic Polling schedule • Enable or disable the Periodic Collection option • Change the Periodic Collection schedule	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Collection Settings
Configuration Management—Archive Management	Setting up the Archive Purge Policy An Audit Trail record is logged any time you make a change in the Archive Purge Setup dialog box.	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Purge Settings
Configuration Management	Setting up the Transport Protocol Order An Audit Trail record is logged any time you make a change in the Config Transport Settings dialog box.	Resource Manager Essentials > Admin > Config Mgmt (Archive Mgmt, Config Editor, NetShow, and NetConfig)

Application Name	Tasks	Navigation
Configuration Management	Setting up the Job Policy An Audit Trail record is logged any time you make a change in the Job Policy dialog box.	Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies (Archive Mgmt, Config Editor, NetShow, and NetConfig)
Device Management	Managing devices in Resource Manager Essentials.	• Resource Manager Essentials > Devices > Device Management > RME Devices • Resource Manager Essentials > Devices > Device Management > Suspended Devices • Resource Manager Essentials > Devices > Device Management > Pre-deployed Devices
Device Management	Deleting devices in Resource Manager Essentials. Also, when a device gets deleted as a result of alias resolution.	• Resource Manager Essentials > Devices > Device Management > RME Devices • Resource Manager Essentials > Devices > Device Management > Normal Devices • Resource Manager Essentials > Devices > Device Management > Pre-deployed Devices • Resource Manager Essentials > Devices > Device Management > Suspended Devices • Resource Manager Essentials > Devices > Device Management > Conflicting Device Types • Resource Manager Essentials > Devices > Device Management > Alias Devices
Device Management	Enabling and disabling these settings in the Device Management Settings window: • Automatically Manage Devices from Credential Repository • Verify Device Credentials While Adding Devices	• Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings
Device Management	Suspending RME devices.	• Resource Manager Essentials > Devices > Device Management > Normal Devices. • Resource Manager Essentials > Devices > Device Management > Pending Devices. • Resource Manager Essentials > Devices > Device Management > Pre-Deployed Devices

Application Name	Tasks	Navigation
Inventory	An Audit Trail record is logged when you: • Create a job for Inventory polling and Inventory collection. • Edit a scheduled job of Inventory polling and Inventory collection. • Cancel the scheduled jobs of Inventory polling and Inventory collection. • Stop the running jobs of Inventory polling and Inventory collection. • Delete the jobs of Inventory polling and Inventory collection.	• Resource Manager Essentials > Devices > Inventory
Inventory	Scheduling a Inventory Polling and Collection Job.	Resource Manager Essentials > Admin > Inventory > System Job Schedule
Inventory	Setting the Inventory Change Filter.	Resource Manager Essentials > Admin > Inventory (Inventory Change Filter)
Reports	Purging Reports Jobs and Archived Reports	Resource Manager Essentials > Admin > Reports
Software Management	Viewing and editing preferences. An Audit Trail record is logged any time you make a change in the View/Edit Preferences dialog box.	Resource Manager Essentials > Admin > Software Mgmt > View/Edit Preferences
Syslog Analysis	Setting up Backup Policy An Audit Trail record is logged any time you make a change in the Backup Policy dialog box	Resource Manager Essentials > Admin > Syslog > Set Backup Policy
Syslog Analysis	Setting the Purge Policy. An Audit Trail record is logged any time you make a change in the Purge Policy dialog box.	Resource Manager Essentials > Admin > Syslog > Set Purge Policy
Syslog Analysis	Performing a Forced Purge An Audit Trail record is logged when a Force Purge job is scheduled.	Resource Manager Essentials > Admin > Syslog > Force Purge
Syslog Analysis	An Audit Trail record is logged when you: • Add an automated action. • Enable or disable the automated actions. • Edit an automated action. • Import the automated actions. • Delete the automated actions.	Resource Manager Essentials > Tools > Syslog > Automated Actions

Application Name	Tasks	Navigation
Syslog Analysis	An Audit Trail record is logged when you: • Create a message filter • Edit a message filter • Enable or disable the filters • Import a filter • Delete a filter • Change message filters type from **drop** to **keep** and vice versa.	Resource Manager Essentials > Tools > Syslog > Message Filters
Syslog Analysis	An Audit Trail record is logged when you subscribe/unsubscribe to a remote syslog collector.	Resource Manager Essentials > Tools > Syslog > Syslog Collector Status
System Preferences	Viewing and editing System Preferences.	Resource Manager Essentials > Admin > System Preferences.
Loglevel Settings	Setting the Loglevels for the Resource Manager Essentials applications.	Resource Manager Essentials > Admin > System Preferences > Loglevel Settings
Editing Device Attributes	Editing the RME device attributes	Resource Manager Essentials > Admin > System Preferences > RME Device Attributes

Note An Audit Trail record is *not* logged for all tasks performed under this navigation **Resource Manager Essentials > Admin > Approval**.

Generating a Standard Audit Trail Report

This option lets you compile a report on all Audit Trail changes that occurred in the network during a specific time period.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate the Standard Audit Trail Report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Audit Trail** from the first drop-down list box.

Step 3 Select **Standard Report** from the second drop-down list box.

Step 4 Enter the information required to generate the required report:

Field	Description
Date Range	
24 Hours	Select this option, only if you want to generate a 24 hours report. This report will contain all the Audit Trail data gathered during the last 24 hours.
From	Click on the calendar icon and select the start date. The From field is enabled only if you have de-selected the 24 Hours check box.
To	Click on the calendar icon and select the end date. The To field is enabled only if you have de-selected the 24 Hours check box.
Selection Criteria	
User Name	Select the user name. This report will be filtered on user names.
Application	Select the name of the application. This report will be filtered on application names.

Step 5 Click **Finish**.

The Audit Trail Standard report appears in a separate browser window.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Understanding the Audit Trail Report

The Audit Trail report contains all change information provided by RME applications based on your filter criteria. It contains the following fields.

Table 15-1 Audit Trail Report

Field	Description
User Name	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the RME application is running, or the name under which the Telnet connection is established.
Application Name	Name of the RME application involved in the network change. For example, ChangeAudit, Device Management, ICServer, NetConfig, NetShow etc.
Server Name	Host name of the RME server.
Creation Time	Date and time at which the changes were performed on the RME server.
Description	Brief summary of the change that occurred on the RME server.

The following buttons are available on the Audit Trail Standard report:

Button	Description
Export to File (Icon)	You can export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Performing Maintenance Tasks

You can either schedule for periodic purge or perform a forced purge of Audit Trail data. This frees disk space and maintains your Audit Trail data at a manageable size.

You can perform these tasks by following this path **Resource Manager Essentials > Admin > Change Audit**

The following sections describe the various tasks which you can perform from Audit Trail:

- Setting the Purge Policy
- Performing a Forced Purge

Setting the Purge Policy

You can specify a default policy for the periodic purging of Audit Trail data.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To set the Audit Trail Purge Policy:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Set Purge Policy**.

The Purge Policy dialog box appears in the Periodic Purge Settings pane.

Step 2 Enter the following information:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged. The default is 180 days. See Tracking Network Changes Using Change Audit for further information.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. The default is 180 days.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the purge job for Change Audit and Audit Trail records. To do this, select one of these options from the drop down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	Enter the start date in the dd Mmm yyyy format, for example, 02 Jun 2004, or click on the calendar icon and select the date.
at	Enter the start time, in the hh:mm:ss format (23:00:00).
Job Info	
Job Description	The system default job description, *ChangeAudit Records - default purge job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Caution You might delete data by changing these values. If you change the number of days to values lower than the current values, messages over the new limits will be deleted.

Step 3 Click **Save**, to save the purge policy that you have specified.

Performing a Forced Purge

You can perform a forced purge of Audit Trail, as required.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To perform a Audit Trail Forced Purge:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Force Purge**.

The Purge Policy dialog box appears.

Step 2 Enter the information required to perform a Forced Purge:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged. See Tracking Network Changes Using Change Audit for further information.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged.
Scheduling	
Run Type	You can specify when you want to run the force purged job for Change Audit and Audit Trail records. To do this, select one of these options from the drop down menu: • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time.
Date	Click on the Calendar icon and select the start date. The Date field is enabled only if you have selected Once as the Run Type.
at	Enter the start time, in the hh:mm:ss format (23:00:00). The At field is enabled only if you have selected Once as the Run Type
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 3 Click **Submit** for the forced purge to become effective.

CHAPTER 16

Checking Bug Status Using Bug Toolkit

Bug Toolkit is an application in Resource Manager Essentials that helps the user identify the bugs filed against devices in their network and check the status of the bugs.

You can generate reports based on bugs filed against IOS and CATOS devices that are managed in the your network.

To generate reports using Bug Toolkit from the CiscoWorks desktop:

Step 1 Select **RME > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Bug Toolkit** from the Select an Application drop down list box.

You can then generate reports using Bug Toolkit.

Bug Summary Report

The Bug Summary Report option allows you to view a summary of the software image bugs for a group of devices.

If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site at www.cisco.com.

To create a Bug Summary report:

Step 1 Select **RME > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Bug Toolkit** from the Select an Application drop down list box.

Step 3 Select **Bug Summary Report** from the Select a Report drop down list box.

Step 4 Select the devices for which you want a summary of outstanding bugs using device selector.

Step 5 Select the hyperlink **Click Here** below the Device Selector to launch the Cisco.com Bug Toolkit.

The Bug Toolkit is launched in a separate browser window where you can view bugs on any Cisco IOS version.

Step 6 Enter the information required to generate a report:

Field	Description	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future.	Select one of the following options from the drop-down list box: Immediate—Runs the report immediately. Once—Runs the report once according to the date and time that you specify. 6–hourly—Runs a job every six hours. 12–hourly—Runs a job every twelve hours. Daily—Runs everyday according to the time that you specify. Weekly—Runs weekly according to the day of the week and the time that you specify. Monthly—Runs monthly according to the day of the month and the time that you specify.
Date	Date on which you want to run the job.	Click on the calendar icon and select the start date. If Run Type is Immediate, the system date is automatically selected.
At	Time when you want to run the job in the future.	Select the hours and minutes from the drop-down lists. If Run Type is Immediate, the system time is automatically selected.
Job Info		
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.	Make each description unique so you can easily identify jobs.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.	Send an e-mail notification when a job is completed.

Field	Description	Usage Notes
Criteria		
Report Bugs From	Displays bugs filed from a particular date.	Select the date from which you wish to run a query.
Cisco.com Profile		
User Name	Cisco.com user name.	Enter your Cisco.com login ID.
Password	Cisco.com password.	Enter your Cisco.com password.

Step 7 Click **Finish**.

The Software Image Bugs Summary Report appears.

Logging Into Cisco.com

To access Cisco.com, login privileges are required. You can login to Cisco.com by entering your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Common Services > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Note Cisco.com account credentials from **Common Services** > **Security** > **Cisco.com Connection Management** > **Cisco.com User Account Setup** and proxy username/password credentials from **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup** will not be used henceforth.

Understanding the Bug Summary Report

The Bug Summary Report is a high-level summary, sorted by device family, of software bugs that apply to your network.

You cannot view device bug details of devices that are not listed in the Cisco.com Bugtoolkit database. The devices not listed in the Cisco.com Bugtoolkit database are listed in the “Device(s) not supported by Cisco.com Bugtool System” row of the Bug Summary Report.

Note The Bug Summary Report is categorized based on device type.

The Bug Summary Reports displays the following information.

Column	Description	Usage Notes
Summary		
Total number of submitted device(s)	Total count of all devices submitted for report generation.	None.
Number of device(s) with Inventory[1] data	Count of devices that contain inventory data in the database.You can generate reports for these devices.	None.
Device(s) without Inventory data	Devices which do not have inventory data in the database. You cannot generate reports for these devices.	None.
Device not supported by Cisco.com Bugtool System	Devices that contain inventory data but do not display a report when the URL is posted to Cisco.com. This may be because Cisco.com does not have data for the device.	None.
Devices timed out	Devices that did not report results because of a connection timeout with Cisco.com.	None.
Bug Toolkit Summary Report		
Device Name	Display name of the device.	None.
Category	Device type of the device.	None.
Image Version	Software version running on a device in your network	None
Image Status	Status of the image running on the device. The status can be: LD — Latest Deployment ED — Early Deployment GD — Global Deployment	None.
Total Bugs[2]	Number of bugs filed against a software release.	Click **digit** to view all bugs.
Catastrophic	Number of catastrophic bugs	Click **digit** to view the list of catastrophic bugs.
Severe	Number of severe bugs	Click **digit** to view the list of severe bugs.

[1] Inventory Data refers to running image filename and image version.

[2] The maximum number of bugs displayed for a device is 2500. 2500 is the Bugtoolkit query limit for a device.

Inconsistencies may occur in the number of bugs displayed in the Bug Summary Report archived in the server and the Bug Details Report information on Cisco.com.

Locate Device Report

The Locate Device Report option allows you to search for known bugs that could affect the devices on your network.

To generate a Locate Device report:

Step 1 Select **RME > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Bug Toolkit** from the Select an Application drop down list box.

Step 3 Select **Locate Device Report** from the Select a Report drop down list box.

Step 4 Enter the information required to generate a report:

Field	**Description**	**Usage Notes**
Bugs Input		
Enter bugs separated by commas	Bug IDs of known problems separated by commas.	Enter the Bug ID. You can enter multiple bug ID with comma separators.
Upload bug list from file	File that contains the list of Bug IDs. The file extension can be anything, but the file should contain the comma separated or space separated or line separated bug list.	1. Click **Browse**. The External Config Selector dialog box appears. 2. Enter the following information: File—Location of the file. For example, D:/CSCOpx Directory content—Name of the directory. For example, \bin Drive—Name of the drive. For example, D:\

Field	Description	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future.	You can specify when you want to run the job. To do this, select one of these options from the drop down menu: • Immediate—Runs the report immediately. • 6- hourly—Runs the report every 6 hours, starting from the specified time. • 12- hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.
Date	Date on which you want to run the job.	Click on the calendar icon and select the start date. If Run Type is Immediate, the system date is automatically selected.
at	Time when you want to run the job in the future.	Select the hours and minutes from the drop-down lists. If Run Type is Immediate, the system time is automatically selected.

Field	Description	Usage Notes
Job Info		
Job Description	Enter job description.	Enter a unique description for each job so that you can easily identify jobs.
E-mail	Allows you to enter the e-mail addresses to which the job will send status notices. Separate multiple addresses with commas.	E-mail notification is sent when job is created, started, deleted, canceled, and completed.
Cisco.com Profile		
User Name	Cisco.com user name.	Enter your Cisco.com login ID.
Password	Cisco.com password.	Enter your Cisco.com password.
Proxy Username	Proxy Username	Enter the Proxy Username
Proxy Password	Proxy Password	Enter the Proxy Password. You are prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in: **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Step 5 Click **Finish**.

Understanding the Locate Device Report

The locate device report contains the following information:

Column	Description	Usage Notes
Summary		
Device(s) with Inventory[1] Data	Devices that contain inventory data in the database. Reports can be generated for these devices.	None.
Device(s) without Inventory Data	Devices which do not have inventory data in the database. Reports cannot be generated for these devices.	None.
Affected Device Report		
Bug ID	Bug identification number	None.
Affected Devices	Names of the devices affected	None.
Headline	Headline of the bug	Click the headline to view the detailed description of the bug.
Found Version	Software version in which the problem was cited.	None

Column	Description	Usage Notes
Fixed Version	Software version in which the problem was resolved.	None
Severity	Severity of the bug	None
Status	State of the bug.	None

---

1. Inventory Data refers to the image version.

CHAPTER 17

Working With SmartCase

SmartCase lets you access Cisco.com from Resource Manager Essentials (RME) to open a Cisco.com case or to query and update an existing case. You can submit, review, and update problems or questions about your Cisco products.

Launching Cisco.com Service Request Tool

SmartCase allows you to Open/Query or Update a case on Cisco.com by launching the Cisco.com Service Request Tool from Resource Manager Essentials.

To launch Cisco.com Service Request Tool:

Step 1 Select **Resource Manager Essentials** > **Tools** > **SmartCase**.

The Open/Query or Update a Case page appears.

Step 2 Click the link provided to launch the Cisco.com Service Request Tool to Open/Query or Update a Case.

The SmartCase.properties file is located at

NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\cctool\scase

The properties file contains the URL used to launch Cisco.com Service Request Tool. If at any time there is a change in this URL, you must go to the properties file and update the URL.

Step 3 Enter your Cisco.com username and password.

You are redirected to the TAC Service Request Tool page.

CHAPTER 18

Working With Contract Connection

Cisco Contract Connection lets you verify which of your Cisco IOS devices are covered by a service contract. Contract Connection (CC) uses Inventory Manager, Cisco.com, and Cisco's internal contract tracking service, Contract Agent, to provide the status of your service coverage.

You must have a Cisco.com account to use CC and CC lists all contracts applicable to you.

You can select any of the contracts to get the contract details for the IOS devices belonging to that particular contract in your network.

Accessing and Using Contract Connection

Contract Connection application allows you to see the status of service contracts of all IOS devices in your network.

To launch Contract Connection:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator page appears.

Step 2 Select **Contract Connection** from the drop-down list box on the left.

Step 3 Select **Report Based on Contract** from the drop-down list box on the right.

The Cisco.com and Proxy Server Credentials Profile dialog box appears as a pop-up.

Step 4 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credentials Profile dialog box.

You must have valid Cisco.com account credentials to generate Contract Connection reports.

- You are also prompted to enter ProxyUsername and ProxyPassword if a Proxy Server hostname/IP and port are configured in:

  Common Services > Security > Cisco.com Connection Management Proxy Server Setup
- After providing the credential information click **OK**.
- A dialog box appears within the Contract Connection Reports page.

Cisco.com account credentials from **Common Services > Security > Cisco.com Connection Management > Cisco.com User Account Setup** and proxy username/password credentials from **Common Services > Security > Cisco.com Connection Management Proxy Server Setup** will not be used hence forth.

Step 5 Enter the name of the device in the Device Names field and click **Select**.

If you enter more than one name, separate the names by commas.

Or

Select the required device from the list tree.

- To see only the devices that you have selected, click **Selection**.
- To see all the devices, click **All.**

Step 6 Select the required contract from the Select Contracts list and click **Finish**.

The Summary Report page appears with a Summary of submitted devices and the Device Type Summary Report for the selected contract.

If you want to revert to the default values in the Contract Connection Reports dialog box, click **Reset**.

Task	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Define/Edit/Delete Contract based on Device Report jobs	Yes	Yes	Yes	Yes	No
View Report Output	Yes	Yes	Yes	Yes	Yes
Set Application level Job Control Policies	Yes	Yes	No	No	No

Getting Device Type Summary Report and Contract Status Detailed Report

The Device Type Summary Report and Contract Status Detailed Report list all the Cisco IOS devices information found on your network. These reports also display any information on the Cisco IOS devices in the Contract Agent.

Device Type Summary Report

The Device Type Summary Report displays the following information:

Field	Description
Product Family	Displays the following: • Product family of the device. • None — Devices that do not belong to Cisco Product Family. • Total — Number of devices managed by Resource Manager Essentials.
Devices on Network	Number of devices managed by Resource Manager Essentials. This also includes devices that do not have a Cisco Contract but are covered by other contracts.
Devices on Contract Total	Number of devices in the contract that you had selected. This also includes devices that are not managed by Resource Manager Essentials.
Devices on Contract Active	Number of active devices in the contract that you selected.

Field	Description
Devices on Contract Expired	Number of expired devices in the contract that you selected.
Devices Matched on Contract Total	Number of devices whose Serial Number in the Resource Manager Essentials inventory, match with the corresponding Serial Number in Cisco support database (Service Contract Center).
Devices Matched on Contract Active	Number of active devices that match in the contract that you selected.
Devices Matched on Contract Expired	Number of expired devices that match in the contract that you selected.
No Serial Number	Number of devices that do not have Serial Numbers. These are devices that do not have both the Electronic Serial Number and the Managed Serial Number.

To view Device Type Summary Report:

Step 1 Select **Resource Manager Essentials** > **Reports > Report Generator**.

The Report Generator page appears.

Step 2 Select **Contract Connection** from the drop-down list box on the left.

Step 3 Select **Report Based on Contract** from the drop-down list box on the right.

The Cisco.com and Proxy Server Credentials Profile dialog box appears as a pop-up.

Step 4 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credentials Profile dialog box.

- You must have valid Cisco.com account credentials to generate Contract Connection reports.
- You are also prompted to enter ProxyUsername and ProxyPassword if a Proxy Server hostname/IP and port are configured in **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Step 5 Enter the credential information and click **OK**.

A dialog box appears within the Contract Connection Reports page.

Cisco.com account credentials from **Common Services** > **Security** > **Cisco.com Connection Management** > **Cisco.com User Account Setup** and proxy username/password credentials from **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup** will not be used henceforth.

Step 6 Enter the name of the device in the Device Names field and click **Select**.

If you enter more than one name; separate the names by commas.

Or

Select the required device from the list tree.

- To see only the devices that you have selected, click **Selection**.
- To see all the devices, click **All.**

Step 7 Select the required contract from the Select Contracts list and click **Finish**.

The Summary Report page appears with a Summary of submitted devices and the Device Type Summary Report for the selected contract.

The Summary displays:

- Total number of submitted devices.
- Number of devices successfully processed by Cisco.com Contract Connection system.
- Devices not processed because of insufficient inventory data, such as vendor type or serial number.

If you want to revert to the default values in the Contract Connection Reports dialog box, click **Reset**.

The following buttons are available in the Summary Report page:

Button	Description
Export to File (Icon)	Exports the report in either PDF or CSV format.
Print (Icon)	Generates a format of the report that you can print.

Contract Status Detailed Report

The Contract Status Detailed Report gives details about a specific device. You can view the following information in the Contract Status Detailed Report page.

Field	Description
Contract Status	Support status for the device. This is determined by a device serial number in the Resource Manager Essentials inventory that matches the serial number in the Cisco support database. The Contract Status can be A=> active, E=> expired or N=> no contract.
Device Type	Cisco-specific device class description.
Device Name	Assigned host name.
Electronic Serial No	Serial number that you set using CLI when you enter the device into the network.
Managed Serial No	Serial number that is in the Resource Manager Essentials inventory database.
Shipment Serial No	Serial number embedded on the chassis hardware.
Contract No	Cisco support contract identification number.
Contract Type	Cisco support contract code.
Cisco Part No	Cisco part number for the device.
Begin Date	Start date of the Cisco support contract for the device. This indicates whether the Contract Status is active or expired.
End Date	End date of the Cisco support contract for the device. This indicates whether the Contract Status is active or expired.
Sales Order	Original device shipment sales identification number.
Ship Date	Date device left Cisco to be delivered to customer.

To view Contract Status Detailed Report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator page appears.

Step 2 Select **Contract Connection** from the drop-down list box on the left.

Step 3 Select **Report Based on Contract** from the drop-down list box on the right.

The Cisco.com Profile dialog box appears as a pop-up.

Step 4 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credentials Profile dialog box.

- You must have valid Cisco.com account credentials to generate Contract Connection reports.
- You are also prompted to enter ProxyUsername and ProxyPassword if a Proxy Server hostname/IP and port are configured in:

  Common Services > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Step 5 Enter the credential information and click **OK**.

A dialog box appears within the Contract Connection Reports page.

Cisco.com account credentials from **Common Services** > **Security** > **Cisco.com Connection Management** > **Cisco.com User Account Setup** and proxy username/password credentials from **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup** will not be used henceforth.

Step 6 Enter the name of the device in the Device Names field and click **Select**.

If you enter more than one name; separate the names by commas.

Or

Select the required device from the list tree.

- To see only the devices that you have selected, click **Selection**.
- To see all the devices, click **All**.

Step 7 Select the required contract from the Select Contracts list and click **Finish**.

The Summary Report page appears with a Summary of submitted devices and the Device Type Summary Report for the selected contract.

The Summary displays:

- Total number of submitted devices.
- Number of devices successfully processed by Cisco.com Contract Connection system.
- Devices not processed because of insufficient inventory data, such as vendor type or serial number.

If you want to revert to the default values in the Contract Connection Reports dialog box, click **Reset**.

Step 8 Click the Product Family name under Product Family in the Device Type Summary Report.

The Contract Status Detailed Report page appears.

- Click **None** to get similar information for devices that do not belong to Cisco Product Family.
- Click **Total** to get the number of devices managed by RME.

The following buttons are available on the Contract Status Detailed Report page:

Button	Description
Export to File (Icon)	Exports the report in either PDF or CSV format.
Print (Icon)	Generates a format of the report that you can print.

Note If the Contract Status Detailed Report page shows no records, press F5 to refresh the page and get the results.

Scheduling Jobs

You can schedule report generation using the Schedule Job option. The job schedule can be Immediate, Once, Weekly or Monthly.

- If you want an Immediate report select the Immediate option.
- If you want reports Once, Weekly or Monthly, specify the time and date on which you want to enable the report collection job.

After the job runs, the status appears in the Job Browser according to the work order.

The generated report is archived separately. The Job Purge Policy is the same as for other reports. For more details on Job Purge Policy, see the topic Purging Reports Jobs and Archived Reports in the Generating Reports section.

To schedule a job:

Step 1 Select **Resource Manager Essentials** > **Reports** > **Report Generator**.

The Report Generator page appears.

Step 2 Select **Contract Connection** from the drop-down list box on the left.

Step 3 Select **Report Based on Contract** from the drop-down list box on the right.

The Cisco.com Profile dialog box appears as a pop-up.

Step 4 Enter your Cisco.com username and password in the Cisco.com and Proxy Server Credentials Profile dialog box.

- You must have valid Cisco.com account credentials to generate Contract Connection reports.
- You are also prompted to enter ProxyUsername and ProxyPassword if a Proxy Server hostname/IP and port are configured in:

  Common Services > **Security** > **Cisco.com Connection Management Proxy Server Setup**

Step 5 Enter the credential information and click **OK**.

A dialog box appears within the Contract Connection Reports page.

Cisco.com account credentials from **Common Services** > **Security** > **Cisco.com Connection Management** > **Cisco.com User Account Setup** and proxy username/password credentials from **Common Services** > **Security** > **Cisco.com Connection Management Proxy Server Setup** will not be used henceforth.

Step 6 Enter the name of the device in the Device Names field and click **Select.**

You can enter more than one name; separate the names by commas.

Or

Select the required device from the list tree.

- To see only the devices that you have selected, click **Selection**.
- To see all the devices, click **All.**

Step 7 Select the required contract from the Select Contracts list.

Step 8 Select the frequency of job scheduling - Immediate, Once, Weekly or Monthly from the Run Type drop down list box.

The date and time are enabled only if you have selected an option other than Immediate in the Run Type field.

Step 9 Click on the calendar icon and select the start date.

Step 10 Select the hours and minutes from the drop-down lists.

Step 11 Enter a description for the job you are scheduling in the Job Description field.

This is a mandatory field, if you have selected Immediate, Once, Weekly or Monthly from the Run Type drop-down list box.

Step 12 Enter your E-mail ID in the E-mail field if you want to be notified when a job is executed.

The mail informs you whether the job was executed successfully or was a failure. You can enter multiple E-mail IDs, separated by commas.

Step 13 Click **Finish**.

A message appears confirming the creation of the job with the Job ID. This message also informs you how you can view the job status from **Reports > Report Jobs**. For example, `Job 1018 was created successfully. Go to Reports > Report Jobs to view the status of the job`.

Step 14 Click **OK**.

Viewing Job Status

To view the status of a job:

Step 1 Select **RME** > **Reports** > **Report Jobs**.

A window appears in the Report Job Browser page. It displays:

- Job ID
- Job Type
- Report Type
- Status
- Description
- Owner
- Schedule Type

Refresh (Icon)	Click this icon to refresh the Report Job Browser.

You can filter by All, Job ID, Job Type, Report Type, Status, Description, Owner, and Schedule Type.

To do this, select the required criteria in the Filter By drop-down list box. Then, select the required report in the drop-down list box. Click **Filter**.

To view Job Details, click on a job number under Job ID.

The Contract Connection Report pop-up window appears with the Job Details.

It contains the Job ID number and status, Job Summary and a Refresh button.

Job Summary displays your E-mail ID or IDs if you had entered it while scheduling the job, Selected Devices, Report Publish Location, Report Name, Selected Contract and the date and time the job was created. Click **OK.**

Step 2 Select the required job in Contract Connection in the Report Job Browser page. You can view the output of successful jobs only.

Step 3 Click **Show output**.

The Summary Report page appears with the Summary of submitted devices and the Device Type Summary Report.

- If you want to stop a scheduled or running job or jobs, select the job and click **Stop** in the Report Job Browser page.
- If the job is a one-time job, a message appears informing you that you are about to delete report jobs(s). Click **OK**.

  A message appears `Successfully stopped the selected job(s)`. Click **OK**.
- If the job is a periodic one, the Period Job Cancel Confirmation dialog box appears after you have clicked **OK** in the dialog box.

  This message informs you that you are about to delete report job(s). It prompts you to confirm whether you want to cancel only this instance or all future instances, as well.

Step 4 Select the option you want and click **OK.**

A message appears `Successfully stopped the selected job(s).`

Step 5 Click **OK**.

If you want to delete a job, click **Delete** in the Job Browser page.

A message appears informing you that you are about to delete report job(s) and no instance will be scheduled in the future. Click **OK**.

A message appears with the job(s) ID informing you that you have successfully deleted the job(s), for example, `Job(s) [1018] deleted successfully`. Click **OK**.

Archiving and Viewing Generated Reports

By default, Contract Connection application archives all generated report for later use, except for Immediate Run Type reports.

For details, see the topic Viewing Archived Reports in the Generating Reports section.

CHAPTER 19

CLI Utilities

Resource Manager Essentials provides Command Line Interface (CLI) support. The CLI utilities that are supported by RME are:

- CWCLI
- Performance Tuning Tool
- .syslogConf.pl Utility
- Software Management CLI Utility

CWCLI

CiscoWorks Command Line Framework (CWCLI) is the interface or framework through which application functionality is provided.

The following are the **`cwcli`** applications:

- **`cwcli config`** is the configuration command-line tool of Resource Manager Essentials. **`cwcli netconfig`** command lets you use NetConfig from the command line.
- **`cwcli export`** is a command line tool that also provides servlet access to inventory, configuration and change audit data.

  This can be used for generating inventory, configuration archive, and change audit data for devices in Resource Manager Essentials (RME).
- **`cwcli inventory`** is a RME Device Management application command line tool. This tool can be used for checking the device credentials, exporting the device credentials. You can also view the RME devices and delete the RME devices.
- **`cwcli invreport`** is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The output is displayed in the (CSV) Comma Separated Value format.
- **`cwcli netshow`** is a comand line tool that lets you use NetShow features from the command line. You can use the cwcli netshow commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

This chapter contains the following sections:

- Overview: CLI Framework (cwcli)
- Overview: cwcli config Command
- Overview: cwcli netconfig Command

- Overview: cwcli export Command
- Overview: cwcli inventory Command
- Overview: cwcli invreport Command
- Overview: cwcli netshow Command

You can set the debug mode for CLIFramework and ConfigCLI in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

See Application Log Level Settings for further details.

Overview: CLI Framework (cwcli)

CLI Framework (`cwcli`) is a Command-Line Interface (CLI). This interface provides application-related functionality.

The CLI Framework supports the following tasks for the RME applications:

- Parsing the command line for the applications.
- Easy logging and messaging capabilities
- Authentication and authorization for individual applications
- Remote access support.

SYNOPSIS

The command line syntax is as follows:

`cwcli` *application command GlobalArgs AppSpecificArguments*

- *application* specifies one or more RME applications that use the framework. For example, config, export, inventory, invreport, and netconfig.
- *command* specifies which core operations are to be performed for a particular service.
- *GlobalArgs* specifies arguments common for all CLI. For example, username, password, log, debug, etc.
- *AppSpecificArguments* are the additional parameters required for each core command.

You should enter the application name immediately after `cwcli` and the command name, after the application name. All other GlobalArgs arguments can be specified in any order.

Apart from the applications, Global args (`-u` *user*, `-p` *password*, `-l` *logfile*, `-m` *email*, `-d` *debuglevel*) framework also supports two generic commands. They are:

- `-v`–Version of the CLI interface.
- `-help`—All the applications that can be invoked using the framework.

SYNTAX

```
cwcli  -v
cwcli  -help
```

cwcli Global Arguments

The following table shows the `cwcli config` command arguments you can specify with all commands.

cwcli arguments	Description
-u *userid*	User ID. Field is required.

-p *password*	It is the password for the specified User ID.
	If you enter the password at the command line, a message appears:
	`* Warning * The -p option is highly insecure and *not* recommended. See -u option for more details.`
	If the password is not specified in the command line, framework searches for the password in the file pointed to by the `CWCLIFILE` environment variable. If the variable is not set, you are prompted to enter the password.
	`* Warning * CWCLIFILE Environment variable not set. Enter your password`
	See Setting CWCLIFILE Environment Variable for more details.

-device *devicename* or *device_list*	Display name of the device added into DCR. You can use comma separated displaynames and wild card character **%**. For example, if there are two devices with names Rtr12 and Rtr13, Rtr% will display both the devices. To use all the devices, use **-device** %.
-view *view_list*	If the data needs to be generated for all the devices in a specific group, you can use the **-view** argument. You can use this argument to generate data for devices in all RME device views including system-defined groups and user-defined groups. You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only. For example, **-view** "/RME@*ciscoworks_servername*/All Devices"
-ipaddress *address*	Device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with **-device**, **-view** , or **-input**. Also, you cannot specify wildcard characters.
-l *logfile*	Must be a relative name. By default ConfigCLI.log and cli.log files under *NMSROOT/log* directories are used. If the relative name is specified then the log messages are logged into the file specified. The file is created under the *NMSROOT/log* directory. For example, **cwcli config export -u** *alpha* **-p** *beta* **-device %** **-l** *export.log*. In this case, export.log is created under the *NMSROOT/log* directory.
-m *email*	Email address to mail the command output to. You can enter single or comma separated email IDs.
-d *debuglevel*	Enables debugging to command-line tool. Specifies debugging verbosity. Default is least verbose.
-help	Displays usage information.
-input	Text file containing arguments for each device.

Note `-d` and `-l` arguments are supported for backward compatibility. In the CiscoWorks LMS Portal home page, select **RME > Admin > System Preferences > Loglevel Settings > CLI Framework** to set debug levels.

When using wildcards, you must use the percent sign (`%`), not an asterisk (`*`), as shown in the following examples:

```
%device (lists all devices that end with the suffix ‘device’)

dev% (lists all devices that start with the prefix ‘dev’)

% (lists all devices RME manages)
```

Remote Access

CLI framework (**`cwcli`**) offers remote access facilities to allow you to invoke **`cwcli`** commands from the client in the same way as they run on the RME server.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

`http://`*rme-server:rme-port***`/rme/cwcli`** *payload XML file*

For get request,

`http://`*rme-server:rme-port***`/rme/cwcli?command=cwcli config`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

Note Use <arg> and <argval> tags when the argument is a file.

The contents of the payload xml file is as follows.

```
<payload>

   <command>

    cwcli config export -u admin -p <Base64Enoced pwd> -device 1.1.1.1 -xml

   </command>

   <arg>

   </arg>

   <arg-val>

   </arg-val>

</payload>
```

For example to execute the **`cwcli config import`** comand payload.xml is as follows:

```
<payload>

   <command>

     cwcli config import -u admin -p <Base64Enoced pwd> -device 10.77.240.106

     <arg>

     -f
     </arg>
     <arg-val>
      tempfile
     </arg-val>
   </command>
</payload>
```

The Remote Access servlet creates a temporary file with the contents specified between the arg-val tags for the **import** command. On the server the command is executed as
cwcli config import -u *admin* **-p** *Base64Enoced pwd* **-device** *10.77.240.106* **-f** *tempfile*

Here, the tempfile contains the configuration of the device that you want to import.

For example,

perl samplescript.pl http(s)://*rme-server:rme-port***/rme/cwcli** *payloadXML*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

Note For the secure mode (HTTPS) the port number is 443. The default port for CiscoWorks server in HTTP mode is 1741.

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{        $str .= $_ ;
}
print $str ;
url_call($temp);
#-- Activate a CGI:
sub url_call
{
my ($url) = @_;
my $ua = new LWP::UserAgent;
$ua->timeout(1000);
# you can set timeout value depending on number of devices
my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
my $req = new HTTP::Request ('POST', $url, $hdr);
$req->content($str);

my $res = $ua->request ($req);

my $result;


if ($res->is_error)

{

print "ERROR : ", $res->code, " : ", $res->message, "\n";        $result = '';

}

else {

    $result = $res->content;

       if($result =~ /Authorization error/)

{           print "Authorization error\n";

          }

else {

print $result ;

         }

     }

}
```

Setting CWCLIFILE Environment Variable

You can store your username and password in a file and set a variable *`CWCLIFILE`* which points to the file, if you want to avoid the **`-p`** argument which will reveal the password in clear text in CLI.

You should maintain this file and control access permissions to prevent unauthorized access.

If *`CWCLIFILE`* is set only to filename instead of full path, **`cwcli`** framework looks for the current working directory.

If you use the **`-p`** argument, even after setting the *`CWCLIFILE`* variable, the password is taken from the command line instead of *`CWCLIFILE`*. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

`username password`

Where username and password are the CiscoWorks login credentials. The delimiter between the username and password is a single space.

You must enter a comma as the delimiter if the password is blank. Otherwise, `cwcli` framework will fail to validate the password.

Example to run the cwcli command with the `CWCLIFILE` file:

On Windows, at the command prompt enter:

```
C:\Program Files\CSCOpx\bin>set CWCLIFILE=D:\ciscoworks\password.txt
```

```
C:\Program Files\CSCOpx\bin>cwcli export changeaudit -u admin -view
"/RME@ciscoworksservername/Normal Devices"
```

Where the file, password.txt contains the username and password for CiscoWorks server.

Overview: cwcli config Command

The `cwcli config` command-line tool performs the following core functions on one or more devices and the configuration archive:

- Moves configuration files from the configuration archive to one or more devices.
- Transfers the configuration files from devices to the archive if the configuration running on a device is different from the latest archived version
- Imports configuration files from the file system and pushes them to one or more devices, which updates the configuration archive
- Merges the startup configuration files with the running configuration files
- Copies the running configuration files to the startup configuration files
- Copies a configuration file to the startup configuration files
- Copies the difference between a configuration file and the running configuration to the running configuration files. This makes the configuration in the file available on the running configuration.
- Reboots running devices to load a running configuration with its startup configuration

In addition, `cwcli config` performs the following core functions on the configuration archive:

- Exports configurations from the archive to the filesystem
- Compares any two configuration files in the archive based on version or date
- Deletes configurations older than a specified date from the configuration archive

Using the cwcli config Command for Batch Processing

In addition to using the graphical-based device configuration functions, you can use the `cwcli config` command-line utility to perform batch processing tasks on the configuration archive, devices, or on both.

For more details see these sections:

- Running cwcli config
- cwcli config Core Arguments
- Examples of cwcli config

On platforms other than Windows 2000, all files created by `cwcli config` are owned by casuser. They belong to the same group as the user (casuser) who created the files, and have read-write access for both casuser and the group.

Note Your login determines whether you can use this argument.

Getting Started With cwcli config

`cwcli config` is a command-line tool. This tool is like an interface between the user and the device and the configuration archive.

Generally, the configuration archive automatically registers modifications to the device's configuration in archived, version-based files. Over time, multiple configurations of a device accumulate in the archive. Typically, the latest version is the configuration running on the device.

Uses of cwcli config

With `cwcli config`, you can:

- Device and Archive Updates

  Modify a device's running configuration. You can allow personnel of your organization to modify the device's configuration without explicitly providing them with Telnet access to the device.
- Deleting Configurations

  Delete unwanted versions of the configuration file from the archive. This is a command-line variant of the UI purge feature.
- Comparing Configurations

  Generate 'diffs' of different configuration versions of the same device to find out what modifications were made. This is a command-line counterpart for GUI-based reports.

Device and Archive Updates

Whenever you use `cwcli config` to update the running configuration of the device, the tool also archives the newly written configuration to the archive, bypassing the auto-detection mechanism.

Getting a Version of the Device Configuration

To obtain a version of the device's configuration from the device, modify it, and then write it back to the device. You use two features of `cwcli config` to do this.

1. Use the `export` command to obtain a copy of the desired configuration version file.
2. Edit and deploy it on the device using the `import` function. If the update succeeds, `import` also archives the configuration in the archive as the latest version.

Example:

```
cwcli config export -u user -p pass -device zebra.domain.com -version 3 -f zebraconf
```

version 3 of device zebra's configuration has been obtained from the device. It is available in the file zebraconf. You must edit the file and make the necessary modifications.

```
cwcli config import -u user -p pass -device zebra.domain.com -f zebraconf
```

The edited file is written back to the device and archive. If there were five configurations originally, a sixth one is now added.

If you want to update the running config on the device, and are certain that the latest archived version is the same as the running config, then you can obtain the latest version as follows:

```
cwcli config export -u user -p pass -device zebra.domain.com -f zebraconf
```

the latest version is copied to file zebraconf.

After writing the edited configuration to the device, you might want to reboot the device. You can do this automatically from `cwcli config` by using the `-reboot` argument to the `import` command:

```
cwcli config export -u user -p pass -device zebra.domain.com -f zebraconf -reboot
```

In addition, you might want to write file zebraconf to both the running as well as the startup configuration. To do this, enter the following command:

```
cwcli config export -u user -p pass -device zebra.domain.com -f zebraconf -save
```

Reverting to Earlier Configuration Version

For running configuration, use either compare or export to decide, which version to revert to.

For VLAN configuration, look into the Configuration Version Report for the device to find the versions for which VLAN configuration is also archived. Then use **`put`** to deploy the desired version.

The **`put`** function gets the requested version from the archive, writes it to the device. For Running configuration, it archives it as the latest version of that device.

Example:

`cwcli config put -u` *user* **`-p`** *pass* **`-device`** *zebra.domain.com* **`-version`** *3*

version 3 of device zebra's configuration is extracted from the archive and written to the device. It is also stored in the archive as the latest version.

Example:

`cwcli config put -u` *user* **`-p`** *pass* **`-device`** *zebra.domain.com* **`-version`** *3* **`-filetype`** *vlan*

version 3 of device zebra's vlan configuration is extracted from the archive and written to the device.

Like **`import`**, the **`put`** function allows you to reboot the device using the **`-reboot`** argument, and to update the startup configuration using the **`-save`** argument.

Writing Startup Configuration to Running Configuration

To write the startup configuration of the device to its running configuration. Use the **`start2run`** function of **`cwcli config`** to retrieve the startup configuration from the device, and then write it back to the device's running configuration. The new running configuration is archived as the latest version.

Example:

`cwcli config start2run -u` *user* **`-p`** *pass* **`-device`** *zebra.domain.com*

To ensure that the running configuration on the device is stored in the archive, that is, synchronize the archive with the device. Use the get function to do so.

Example:

`cwcli config get -u` *admin* **`-p`** *admin* **`-device`** *zebra.domain.com*

The running configuration of device zebra is retrieved from the device and archived as the latest version, only if there is a need to do so. However, if the running configuration does not differ from the latest archived version, then the archival does not take place.

Configuration updates can be performed on multiple devices at once. For more details see "Running cwcli config on Multiple Devices" section on page 19-10.

Deleting Configurations

Use the **`delete`** function of **`cwcli config`** to delete unwanted versions from the archive, to conserve disk space, and to reduce visual clutter on reports.

Example:

`cwcli config delete -u` *user* **`-p`** *pass* **`-device`** *zebra.domain.com* **`-version`** *2 5*

All versions between and including 2 and 5 are removed from the archive. There is also a time-stamp based variant.

Comparing Configurations

Use the `compare` function to compare any two versions of the archived configuration files of one or more devices. The compare function also lists down the entire configuration changes based on the timestamp.

Example:

```
cwcli config compare -u user -p pass -device zebra.domain.com -version 2 5
```

`cwcli config` can only compare the archived configuration files. The compliance report is stored in the job directories.

Remote Access

`cwcli config` uses remote access facilities offered by the CLI framework to allow you to invoke the `cwcli config` commands from the client in the same manner they would execute them on the RME server.

The name of the servlet is /rme/cwcli.

All the command can be executed remotely.

Note For the secure mode (HTTPS) the port number is 443. The default port for CiscoWorks server in HTTP mode is 1741.

Running cwcli config

The `cwcli config` command is located in the following directories, where install_dir is the directory in which RME is installed:

- On UNIX systems, /opt/CSCOpx/bin
- On Windows systems, install_dir\CSCOpx\bin

  The default install directory is C:\Program Files.

If you install RME on Windows on an NTFS partition, only users in the administrator or casuser group can access `cwcli config`.

Users with read-execute access to the CSCOpx\files\archive directory and the directories under that can also use `cwcli config`.

Running cwcli config on Multiple Devices

You can run `cwcli config` simultaneously on multiple devices. Details vary from command to command. This section describes how to apply import on multiple devices. Details of multiple-device syntax for other commands are described under the DESCRIPTION in the man page.

The commands, such as `put`, `import`, `write2run` and `write2start` accept only one device on the command line. If you want to apply the command to multiple devices, enter the names of those devices and any arguments in a text file.

For example, assume that you want to deliver the configuration file serviceconf to devices, antelope and rhino. Also assume that you want to reboot rhino. The command line of `cwcli config` is as follows:

```
cwcli config import -u admin -p admin -input device-list -m root@netcontrol.domain.com
```

You do not want the output of the command to go to stdout. Instead, you want it to be mailed to the superuser at host netcontrol device-list is a text with the following contents:

```
# comments start with a leading hash symbol. Write serviceconf to rhino and # antelope.
reboot antelope.

-device rhino.domain.com -f serviceconf

-device antelope.domain.com -f serviceconf -reboot


# end of input file device-list
```

Additional Information

The examples in this man page are not comprehensive. There are many other scenarios in which **`cwcli config`** can be used.

For example, if you want to modify the running configuration on the device, without using the latest archived version, considering the latest may not be the same as the running configuration. You can apply the get command and then export and import. Various combinations of the features can be used.

You can also use **`cwcli config`** in UNIX cron jobs to schedule config updates in advance.

Also, the output generated by **`cwcli config`** can be logged to a file and sent to any recipient through email. A host of additional arguments can be applied on other commands.

cwcli config Command Parameters

Using the **`cwcli config`** commands you can manipulate, deploy and archive your device configuration files.

- Using the Compare Command
- Using the Delete Command
- Parameters For All cwcli config Commands
- cwcli config Syntax Examples

Using the Compare Command

When you specify the **`compare`** command, both **`-version`** and **`-date`** are optional.

- If you do not specify **`-version`** or **`-date`**, the latest configuration is compared with the previous version.
- If you do specify **`-version`** or **`-date`**, and the value you enter is the latest version or date, that configuration is compared with the previous version.

Using the Delete Command

When you specify the **`-date`** command, you must specify **`-version`** or **`-date`**.

If you specify only one date, all versions archived up and including that date are deleted.

To delete a version archived on a particular date, specify two dates that are the same date as the archived version date. The latest two versions of configuration can never be deleted from the archive. Be careful while using the **`delete`** command.

Parameters For All cwcli config Commands

The **`-d`** and **`-l`** arguments are supported for backward compatibility.

In the CiscoWorks LMS Portal home page, select **Resource Manager Essentials > Admin > SystemPreferences > Loglevel Settings > ConfigCLI** to set debug levels.

When using wildcards, you must use the percent sign (%), not an asterisk (*), as shown in the following examples:

```
%device
```

```
dev%
```

```
%device%
```

The following table lists the **`cwcli config`** command-specific arguments and which commands you can use the arguments with:

cwcli config arguments	Applicable Commands	Description
`-baseline`	**`createdeployparamfile`**, **`directbaselinedeploy`**	Specifies the name of the Baseline template for which the parameter file has to be created.

`-date`	**`compare`**, **`delete`**	- Compare
		  – If you specify one date, the latest configuration version is compared with the most recently archived version on that particular date.
		  – If you specify two dates, the most recently archived version of the first date is compared with the most recently archived version of the second date.
		- Delete
		  – If you specify one date, all versions archived up to this date are deleted.
		  – If you specify two dates, all versions archived between and on those dates are deleted.

`-enable_pass`	**`import`**, **`put`**, **`write2run`**, **`write2start`**, **`run2start`**, **`start2run`**, **`deploycomplianceresults`**, **`compareanddeploy`**, **`reload`**	Specifies execution mode Base64 encoded Password for connecting to device.
`-f` *filename*	**`export`**, **`import`**	Specifies fully qualified pathname of configuration file to import to or export from. - If you do not specify this argument, the current working directory is assumed. - If you do not specify this argument when importing or exporting a single device configuration, default filename, devicename.cfg, in the current working directory is assumed. The **`-f`** argument applies only to single devices. To perform the operation on multiple devices, you must specify the **`-input`** argument.

cwcli config arguments	Applicable Commands	Description

-input *inputlist*	Applicable to all commands except **compareanddeploy**, **createdeployparamfile**, **deploycomplianceresults**, and **directbaselinedeploy**,	You must enter **-input** inputlist to run commands, such as put and import, on multiple devices.
		The parameter, inputlist is a text file containing arguments for each device. A line starting with # is treated as a comment.
		For example, an input list file might look like this:
		`#comment line`
		`-version version [-save] [-reboot] device_name`
		`-version version [-save] [-reboot] device_name`

-jobid	**createdeployparamfile**	Used to specify the job identifier of the previously executed comparewithbaseline job.
-l	**createdeployparamfile**, **directbaselinedeploy**	Specifies the file to log the results of the command.
-listonly	**write2run**	Displays difference between the latest running configuration for device in configuration archive and new configuration that is generated, without downloading changes.
-m	**createdeployparamfile**, **directbaselinedeploy**	Specifies an email address to send the results of the command.
primary_pass	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **deploycomplianceresults**, **compareanddeploy**, **reload**	Specifies primary user name for connecting to device.
-primary_user	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **deploycomplianceresults**, **compareanddeploy**, **reload**	Specifies primary user name for connecting to device.
-reboot	**import**, **put**	After successfully pushing a configuration to a device, device reboots. By default the device does not reboot. For IOS devices, you must also specify -save to avoid losing configuration changes when rebooting.
-save	**import**, **put**	Applies to Cisco IOS devices only. Performs a write memory after pushing the configuration. The default is no write memory.

cwcli config arguments	Applicable Commands	Description
-timeout	**import**, **put**, **write2run**, **write2start**, **run2start**, **start2run**, **comparewithbaseline**, **deploycomplianceresults**, **compareanddeploy**, **get**, **reload**	Specifies the duration of the interval in seconds between two successive polling cycles. Archive management is polled according to the interval specified to retrieve and display the job results.
-version *version*	**compare**, **delete**, **export**, **put**	• For put and **export**, you can specify one version of the configuration in the archive. • For compare, you can specify two versions, which are compared with each other. If you specify only one version, that is compared with latest archived version. • For delete, if you specify one version, that version is deleted. If you specify two versions, all versions in between and including those version are deleted.

cwcli config Syntax Examples

The following examples demonstrate the **`cwcli config`** command syntax. Square brackets ([ ]) indicate arguments. A pipe (|) acts as a delimiter. This means that only one of the listed entries can be specified.

Note Make sure you first use the **`cwcli config`** command in a test environment before running the command in production. This is to avoid any loss of data when a device is rebooted or a configuration is overwritten.

The following command extracts the running configurations from all devices:

```
cwcli config get -u user -p password -device %
```

The following command exports the configuration of all the devices from the archive and puts the configuration into the file, devicename.cfg. This is the default file name because **`-f`** is not specified:

```
cwcli config export -u user -p password -device %
```

If there is more than one device in the default view All, you see an error message because the **`export`** command does not accept multiple device names on the command line. You must specify the **`-input`** argument to run the **`export`** command on more than one device.

The following table shows more syntax examples:

Argument	Syntax	Notes
no arguments	**cwcli config -u** *user* **-p** *password* [**-v -help**]	If you do not specify arguments, **cwcli config** shows command usage (**-help**)
compare	**cwcli config compare -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] }	Specify versions to compare using **-version** or **-date** argument. When specifying a date, use format mm/dd/yyyy. If you do not specify a date or a version, the latest two archived configurations are compared.
compareanddeploy	**cwcli config compareanddeploy -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] {**-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance.
comparewithbaseline	**cwcli config comparewithbaseline -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*]	Creates a job that compares the given Baseline template with the latest version of the configuration for a device. In case of non-compliance, the non-compliant commands are displayed.
delete	**cwcli config delete -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] }	Deletes the specified device configuration from the archive. Use **-date** or **-version** argument to specify configurations to delete. If you specify two dates, all configurations archived between those dates are deleted. If you specify two versions, all configurations between and including the versions are deleted.
deploycomplianceresults	**cwcli config deploycomplianceresults -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-substitute** *datafile* } {**-jobid** *jobID*}[**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that uses the previously executed **comparewithbaseline** job to get the non-compliance commands and create a job. It replaces the parameters in the non-compliant commands with the values from the data file. The commands are then downloaded to ensure compliance with the baseline configuration.
export	**cwcli config export -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *displayName* **-view** *name* | **-ipaddress** *list* } [**-f** *filename*] [**-version** *number*] [**-xml**] [**-input** *argumentFile*]	Retrieves a configuration version for a device from the archive and writes it to a file. Exported configurations are named devicename.cfg if **-f** argument is not used.

Argument	Syntax	Notes
get	**cwcli config get -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*][**-timeout** *seconds*] [**-filetype** *running|startup|runningstartup*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }	Creates a job that fetches the configuration from the device and stores it in the archive.
import	**cwcli config import -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*][**-timeout** *seconds*] { **-device** *displayName* |**-ipaddress** *address* } [**-f** *filename*] [**-save** [**-reboot**]][**-input** *argumentFile*]	Creates a job that retrieves the configuration from a file and transfers it to the device. The job is added to the device running configuration. It then polls Archive Management at periodic intervals to get the job results and display it. Specify **-input** to operate on more than one device. You cannot specify wildcards or more than one device.
listversions	**cwcli config listversions -u** *userid* **-p** *password* [**-d** **debuglevel**] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *displayName* **-viewname** | **-ipaddress** *list*} **-baseline**	Lists the versions of the configuration archived for a device on the main branch or the Baseline templates applicable to a device.
put	**cwcli config put -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *displayName* |**-ipaddress** address **-version** *number*}[**-config** *1|2*][**-save** [**-reboot**]] [**-input** *argumentFile*][**-timeout** *seconds*] [**-filetype** *vlan|running*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]]	Creates a job that retrieves the configuration from the configuration archive and pushes it to the device. Specify **-input** to operate against more than one device. You cannot specify wildcards or more than one device. You must specify a version.
reload	**cwcli config reload -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }[**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that reboots devices. The configuration loaded runs with the startup configuration.
run2start	**cwcli config run2start -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*]{ **-device** list | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list*}[**-config** 1|2] [**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that overwrites the startup configuration of device with running configuration. Specify multiple devices with **-device** argument by separating each device name with comma or with **-input** argument, which takes filename containing the multiple devices as an argument.

Argument	Syntax	Notes
start2run	**cwcli config start2run -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } [**-config** 1|2] [**-input** *argumentFile*][**-timeout** *seconds*] [**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that merges the startup configuration with running configuration. Specify multiple devices with **-device** argument by separating each device name with comma or with **-input** argument, which takes filename containing the multiple devices as an argument.
write2run	**cwcli config write2run -u** *userid* **-p** *password* [**-d** *debuglevel*][**-m** *email*][**-l** *logfile*] { **-device** *displayName* | **-ipaddress** *address* } **-f** *filename* [**-config** *1*|2][**-listonly**][**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*][**-primary_pass** *Base64 encoded primary password*][**-enable_pass** *Base64 encoded enable password*]	Creates a job that downloads the differences between the specified file and the latest version in the archive for the specified device. If you specify **-listonly**, difference is displayed but no changes are downloaded. To run command on multiple devices, use **-input** argument, which takes a filename as an argument.
write2start	**cwcli config write2start -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *displayName* |**-ipaddress** *address* **-f** *filename*} [**-config** 1|2][**-input** *argumentFile*][**-timeout** *seconds*][**-primary_user** *primary user name*][**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*]	Creates a job that erases contents of device startup configuration and writes contents of given file as new startup configuration. You must specify a filename. To run a command against multiple devices, use **-input** argument.

cwcli config Core Arguments

cwcli config Argument	Description
compare	Compares last two configurations in archive, specific configuration versions, or configuration changes based on a specified date. To run this command on multiple devices, specify **-device** argument or **-input** argument.
delete	Deletes configurations older than specified date or version from archive. To run this command on multiple devices, specify **-device** argument or **-input** argument.
export	Retrieves latest configuration from archive and writes it to specified file. To run this command on multiple devices, specify **-input** argument.
get	Pulls configuration from device to configuration archive if configuration is different from latest archived configuration. To run this command on multiple devices, specify **-device** argument or **-input** argument.

cwcli config Argument	Description
`import`	Imports configuration from specified file and pushes it to devices. To run this command on multiple devices, specify `-input` argument.
`put`	Pushes configuration files from RME configuration archive to device based on version. To run this command on multiple devices, specify `-input` argument.
`reload`	Reboots devices to reload running configuration with startup configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`run2start`	Overwrites startup configuration with running configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`start2run`	Merges startup configuration with running configuration. To run this command on multiple devices, specify `-device` argument or `-input` argument.
`write2run`	Downloads difference between latest running configuration for the device in configuration archive with configuration in file specified by -f argument. To run this command on multiple devices, specify `-input` argument.
`write2start`	Erases the contents of the device's startup configuration and writes the contents of the given file as the device's new startup configuration. To run this command on multiple devices, specify `-input` argument.

Examples of cwcli config

The following `cwcli config` command retrieves configurations for all devices in the CiscoWorks home_routers domain and stores the configurations in Sybase:

```
cwcli config get -u adam -p max -view home_routers
```

where home_routers is an RME device view.

The following `cwcli config` command reads inputfile and, for each device listed, pushes the appropriate configuration to that device:

```
cwcli config import -U adam -P max -input /tmp/inputfile
```

cwcli config Command Man Page

This man page is also accessible from the command line of a CiscoWorks server installed on a UNIX system.

To view the man page, add the path install_dir/CSCOpx/man to the MANPATH variable. Then you can enter the command man `cwcli config` from any directory.

You can also access man pages for each `cwcli config` command by entering the command man cwc-command, where command is the command name (for example, `export`).

The man pages for each subcommand are also available in this help system.

NAME

`cwcli config` CiscoWorks command line interface for the device configuration archive

SYNOPSIS

cwcli config *command* {**-arg1** [*arg1Value*] **-arg2** [*arg2Value*] **-argN** [*argNValue*]}

cwcli config -help

DESCRIPTION

cwcli config is a CiscoWorks command line tool that allows you to access the configuration archive or configurations on devices. You can use **cwcli config** to update, export, and import configurations on devices and in the archive. You can also compare configurations and delete old configurations.

To get a list of supported commands, run the command

cwcli config -help

or

cwcli config?

Help on each command can be obtained in the following manner:

cwcli config *command* **-help**

For example:

cwcli config export -help

Additionally, man pages are available on UNIX installations for individual commands. To view the man page for any command, enter:

man cwc-*command*

For example:

man cwc-export

Arguments

Many of the arguments are common across all commands. These arguments can be broadly classified as those that are expected by every command (function independent) and those that are specific to the context of a command.

- Mandatory Arguments
- Function-independent Arguments
- Function-dependant Arguments
- Function-specific Arguments
- Common Arguments
- Command Arguments

Mandatory Arguments

You must use the following arguments with all commands.

-u *userid*

Specifies the CiscoWorks username. You must define an environment variable `cwcli CWCLIFILE` with value set to a filename, which will contain the corresponding password.

The file has to be maintained by you. You can control the access permissions of this file to prevent un-authorized access. **cwcli config** looks for current working directory if `cwcli CWCLIFILE` is set to only file name instead of full path.

If **-u** argument is used along with **-p** argument, the password is taken from the command line instead of `cwcli` *`CWCLIFILE`*. This is not secure and usage of this argument is not recommended.

The password must be provided in the file in the following format:

```
username password
```

Where username is the CiscoWorks user name given in command line. The delimiter between username and password is single blank space. You must provide the delimiter if the password is blank

Otherwise, **`cwcli config`** will not validate the password. The password file can contain multiple entries with different user names. The password of the first match is considered in case of duplicate entries.

See Setting CWCLIFILE Environment Variable for more details.

Function-independent Arguments

You can use the following arguments without any commands:

`-help`

When run with the **`-help`** argument, **`cwcli config`** displays a list of all supported commands and a one-line description of the command.

`-v`

When run with the **`-v`** argument, **`cwcli config`** displays **`cwcli config`** version information.

Function-dependant Arguments

You can use the following arguments only with commands:

`-p` *password*

Specifies the password for the CiscoWorks username.

Warning **SECURITY WARNING: If -p *password* is used, the password is read from the command line instead of `cwcli CWCLIFILE`. This is highly insecure and *not* recommended. See -u argument for more details. See Setting CWCLIFILE Environment Variable for more details.**

`-d` *debuglevel*

Sets the debug level based on which debug information is printed. debuglevel is a numeric value between 1 and 5.

`-f` *filename*

Specifies the name of the file to which the retrieved configuration is written. If not specified, devicename.cfg is assumed.

`-l` *logfile*

Logs the results of the **`cwcli config`** command to the specified log filename.

`-m` *mailbox*

Mails the results of the **`cwcli config`** command to the specified email address.

Function-specific Arguments

You can use the following arguments only with specific commands:

`-baseline`

Used with the **`compareanddeploy, deploycomplianceresults, listversions, createdeployparamfile, directbaselinedeploy,`** or **`comparewithbaseline function`**, specifies the name of the Baseline template that is compared with the latest configuration version of the device.

If there are commands in the baseline configuration file that are not compliant with the latest configuration of the device in the archive, they are downloaded to the device.

Note The Baseline template must not contain any parameters for the command to succeed.

`-date` *date1 date2*

Used with the **`compare`** or **`delete`** command, specifies the configuration date(s) to compare or delete. Use the format mm/dd/yyyy.

`-device` *name*

Used with the **`export, import,`** or **`put`** function, specifies the name of the device. You can specify a wildcard, %, in the device name to match any device(s) that have the same textual pattern.

`-device` *list*

Used with the **`get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run`** or **`delete`** commands

Specifies the list of device names separated by commas. You can specify a wildcard, %, in the device list to match device(s) that have the same textual pattern.

`- ipaddress` *list*

Used with the **`get, start2run, compare, compareanddeploy, comparewithbaseline, deploycomplianceresults, listversions, put, run2start, start2run, write2run`** or **`delete`** commands.

Specifies IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.

You cannot use this option with **`-device`**, **`-view`**, or **`-input`**. Also, you cannot specify wildcard characters.

`-filetype` *type*

Used with the put function, specifies the type of the configuration (running/vlan) that should be written to the device.

`-f` *filename*

Used with the **`directbaselinedeploy, export, import, write2run or write2start function`**, specifies the name of the file to which the configuration from archive should be exported to. Used with the **`import`** function, specifies the name of the file that contains the configuration to import.

Note **`-f`** argument must not be specified when **`-view`** or **`-device`** % is used. If used, the given file will be overwritten with the configuration retrieved for other devices.

`-input` *listfile*

Used with the **`export, import, compareanddeploy, comparewithbaseline, deploycomplianceresults`** or **`put`** function, specifies the name of the file containing the arguments for multiple devices.

The contents of the file must be similar to those described in the Input List File Format section later in this man page.

`-listonly`

Used with the **`write2run`** function, lists the differences between the running configuration and the specified configuration file.

`-reboot`

Used with the **`import`** or **`put`** function, reboots the device after the configuration has been written to the device.

`-save`

Used with the **`import`** or **`put`** function, saves the configuration written to the device to the device's memory.

`-timeout`

Used with the **`compareanddeploy, deploycomplianceresults, import, put, run2start, start2run, write2run`** or **`comparewithbaseline`** function, specifies the duration of the interval in seconds between two successive polling cycles.

`-version number`

Used with the **`export`** function, specifies the configuration version to retrieve from the archive. Used with the put function, specifies the configuration version to load from the archive and push to the device.

`-version` *version1 version2*

Used with the **`compare`**, or **`delete`** function, specifies the configuration version(s) to compare or delete.

`-view` *name*

Specifies the device view where the device name specified with **`-device`** argument is located. If **`-device`** argument is not specified, performs the operation on all devices in the view. More details are described in the **`-view`** Argument Usage section later in this man page.

`-xml`

Creates an XML file with the name of the device containing the configuration retrieved.

Input List File Format

For commands that do not accept multiple device names on the command line, such as put, **`import`**, and **`export`**, you can create an input list file that contains a list of devices to perform the operation on.

The contents of the input list file are a sequence of lines. Each line specifies a device name and the arguments to apply to that device. The arguments must be specific to the function. You cannot include view names in the input list file. You must specify view names on the command line. You can include comments in the input list file by starting the each commented line with #.

Input List File Example:

For the command

`cwcli config put -u` *userid* **`-p`** *password* **`-view`** *myView* **`-input`** *~/todo_list*

An example of the input list file ~/todo_list is # Comment line.

```
-version 3 -reboot -device enm-2501.cisco.com
-version 2 -save -device enm-4500.cisco.com
```

-view Argument Usage

If both **`-device`** and **`-view`** are specified, the devices in that view and the devices specified against **`-device`** are considered.

For example, assume that **`-view`** has two devices D1 and D2 and D3 is specified against **`-device`**, then all the three devices D1, D2 and D3 are considered.

`-view` Argument Usage Examples:

Search for a device in a specified view:

```
cwcli config export -u admin -p admin  -view myView -device myDevice
```

cwcli config Subcommand Man Pages

Each **`cwcli config`** command has a man page. You can access these man pages from the command line of a CiscoWorks server installed on a UNIX system.

To view the man pages, add the path:

`install_dir/CSCOpx/man` to the *MANPATH* variable.

Then you can enter the command
`man cwc-` *command*

where *command* is the command name. For example, export.

This topic contains the man pages for the following **`cwcli config`** subcommands:

- compare
- comparewithbaseline
- compareanddeploy
- delete
- deploycomplianceresults
- export
- get
- import
- put
- reload
- run2start
- start2run
- write2run
- write2start
- listversions
- createdeployparamfile
- directbaselinedeploy

compare

Name	**`cwcli config compare`** – CiscoWorks **`cwcli config compare`** function
Syntax	**`cwcli config compare -u`** *userid* **`-p password`** [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] { **`-device`** *list* | **`-view`** *name* | **`-device`** *list* **`-view`** *name* | **`-ipaddress`** *list* } { **`-version`** *version1* [*version2*] | **`-date`** *date1* [*date2*] } **`cwcli config compare -help`**
Description	**`compare`** lists the differences between versions of a device configuration. You can specify the versions to be compared by using the **`-version`** argument or the **`-date`** argument. • If you specify the **`-version`** argument with only one version number, that version is compared with the latest archived configuration of the device. • If you specify the **`-date`** argument with only one date, the configuration version with that date is compared with the latest archived configuration. When specifying a date, use the format mm/dd/yyyy. • If you do not specify either a date or a version, the latest two archived configurations are compared. You can specify multiple devices by separating each device name with a comma. The output of the Compare function can be interpreted as follows: – Lines preceded by '+' sign signify those occurring only in the first version but not in the latter. – Lines preceded by '-' sign signify those occurring only in the latter version but not in the first. – Lines preceded by '<' and '>' connote those which are present in both files but differ from each other.

compareanddeploy

Name	**`cwcli config compareanddeploy`** – CiscoWorks compare and download configuration with Baseline template function.
Syntax	**`cwcli config compareanddeploy -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*][**`-l`** *logfile*] { **`-device`** *list* | **`-view`** *name* | **`-device`** *list* **`-view`** *name* |**`-ipaddress`** *list* }{ **`-baseline`** *baselinefile* }[**`-timeout`** *seconds*] [**`-input`** *argumentFile*] [**`-primary_user`** *primary user name*] [**`-primary_pass`** *Base64 encoded primary password*] [**`-enable_pass`** *Base64 encoded enable password*] **`cwcli config compareanddeploy -help`**
Description	**`compareanddeploy`** creates a job that compares the given Baseline template with the latest version of the configuration for a device and downloads the configuration to the device if there is non-compliance. If you specify **`-baseline`** argument, the name of the Baseline template is compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. **Note** The Baseline template must not have any parameters for the command to succeed.

comparewithbaseline

Name	**cwcli config comparewithbaseline** - CiscoWorks compare configuration with Baseline template function.
Syntax	**cwcli config comparewithbaseline -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* |**-ipaddress** *list* }{ **-baseline** *baselinefile* }[**-timeout** *seconds*] [**-input** *argumentFile*] **cwcli config comparewithbaseline -help**
Description	**comparewithbaseline** creates a job that compares the given Baseline template with the latest version of the configuration for a device. If you use the **-baseline** argument, the name of the Baseline template is compared with the latest configuration version of the device.

delete

Name	**cwcli config delete** – CiscoWorks **cwcli config delete** function
Syntax	**cwcli config delete -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] { **-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **-ipaddress** *list* } { **-version** *version1* [*version2*] | **-date** *date1* [*date2*] } **cwcli config delete -help**
Description	**delete** deletes the specified device configuration from the archive. You can use the **-date** argument or the **-version** argument to specify which configurations to delete. • If you specify two dates, all configurations archived between those two dates are deleted. • If you specify only one date, all configurations up to and including the configuration archived on that date are deleted. • If you specify two versions, all configurations between and including the two versions are deleted. • If you specify only one version, the configuration corresponding to that version is deleted.

deploycomplianceresults

Name	**cwcli config deploycomplianceresults** - CiscoWorks deploy command with baseline function.
Syntax	**cwcli config deploycomplianceresults -u** *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*][**-l** *logfile*] { **-substitute** *datafile* } {**-jobid** *jobID*}[**-timeout** *seconds*][**-primary_user** *primary user name*] [**-primary_pass** *Base64 encoded primary password*] [**-enable_pass** *Base64 encoded enable password*] **cwcli config deploycomplianceresults -help**
Description	**deploycomplianceresults** uses the previously executed **comparewithbaseline** job to get the non-compliance commands and creates a job after replacing the parameters if any in the non-compliance commands with the values from the data file and then downloads those commands to ensure the compliance with the baseline config. If you specify the **-baseline** argument, the name of the Baseline template which will be compared with the latest configuration version of the device.

export

Name	**`cwcli config export`** – CiscoWorks **`cwcli config`**'s **`export`** function.
Syntax	**`cwcli config export -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] { **`-device`** *name* | **`-view`** *name* | **`-device`** *name* **`-view`** *name* |**`-ipaddress`** *list* } [**`-f`** *filename*] [**`-version`** *number*] [**`-xml`**] [**`-input`** *argumentFile*] **`cwcli config export -help`**
Description	**`export`** retrieves the configuration specified by the **`-version`** argument, for the device specified by **`-device`** and/or **`-view`** argument, from the archive and writes it to the file specified by the **`-f`** argument. • If you do not specify a version number, the latest configuration of the device from the archive is retrieved. • If you do not specify a file name, a file named devicename.cfg is created. To run this command against multiple devices, you must specify the **`-input`** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of the **`cwcli config`** man page.

get

Name	**`cwcli config get`** – CiscoWorks **`cwcli config`** get function
Syntax	**`cwcli config get -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] **`-filetype`** *running|startup|runningstartup* **`-device`** *list* | **`-view`** *name* | **`-device`** *list* **`-view`** *name* | **`-ipaddress`** *list* } **`cwcli config get -help`**
Description	**`get`** retrieves the running configuration from the device(s), specified by the **`-device`** and/or **`-view`** argument, and pushes it to the configuration archive if the running configuration is different than the latest version in the archive. For devices that support vlan configuration like CatIOS devices, the vlan configuration is also fetched and archived along with running-configuration. However, if a new version of the running configuration is not archived, the vlan configuration fetched, overwrites the previously archived vlan configuration for the latest version of running configuration in the archive. You can run the get function against multiple devices by separating each device name with a comma.

import

Name	**`cwcli config import`** – CiscoWorks **`cwcli config import`** function
Syntax	**`cwcli config import -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*][**`-timeout`** *time*] { **`-device`** *name* |**`-ipaddress`** *address*} [**`-f`** *filename*] [**`-save`** [**`-reboot`**]][**`-input`** *argumentFile*] **`cwcli config import -help`**
Description	**`import`** retrieves the configuration from a file specified by the **`-f`** argument, and pushes it to the device specified by the **`-device`** and/or the **`-view`** argument, adding to the device's running configuration. • If you do not specify a file name, a file named device name.cfg is used. You can specify the **`-save`** and **`-reboot`** arguments, which operate the same as for the put argument. To run the **`import`** argument against more than one device, you must specify the **`-input`** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **`cwcli config`**(1). The configuration archive might be updated after you specify the **`import`** argument if the loaded configuration is different from the latest configuration in the archive.

put

Name	**`cwcli config put`** – CiscoWorks **`cwcli config`** put function
Syntax	**`cwcli config put -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] { **`-device`** *name* |**`-ipaddress`** *address* **`-version`** *number*}[**`-config`** *1*|2][**`-save`** [**`-reboot`**]] [**`-input`** *argumentFile*][**`-timeout`** *seconds*] [**`-filetype`** *vlan*|*running*][**`-primary_user`** *primary user name*] [**`-primary_pass`** *Base64 encoded primary password*] [**`-enable_pass`** *Base64 encoded enable password*]] **`cwcli config put -help`**
Description	**`put`** retrieves the configuration specified by **`-version`** from the configuration archive and pushes it to the device specified by the **`-device`** and/or **`-view`** argument The **`-filetype`** can be used to specify the type of configuration viz running/vlan configuration. By default, the running configuration is considered • In case of running configuration, the archived running configuration is merged with the running configuration on the device unless you specify **`-save`**, in which case, the archived configuration is also written to the device's memory. • In case of vlan configuration, the archived vlan configuration overwrites that on the device. The vlan configuration will not come into effect until the device is rebooted. You can specify **`-reboot`** to reboot the device after the configuration (running/vlan) is pushed to the device. To run the put command on more than one device at a time, you must use the **`-input`** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **`cwcli config`**(1).

reload

Name	`cwcli config reload` – CiscoWorks `cwcli config` **reload** function
Syntax	`cwcli config reload -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*] { `-device` *list* | `-view` *name* | `-device` *list* `-view` *name*|`-ipaddress` *list* }[`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*] `cwcli config reload -help`
Description	`reload` reboots the device(s), specified by the `-device` and/or `-view` argument, resulting in the running configuration being loaded with its startup configuration. You can specify multiple devices with the `-device` argument by separating each device name with a comma.

run2start

Name	`cwcli config run2start` – CiscoWorks `cwcli config run2start` function
Syntax	`cwcli config run2start -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*]{ `-device` *list* | `-view` *name* | `-device` *list* `-view` *name* | `-ipaddress` *list*}[`-config` *1|2*] [`-input` *argumentFile*][`-timeout` *seconds*][`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*] `cwcli config run2start -help`
Description	`run2start` overwrites the startup configuration of any device(s), specified by the `-device` and/or `-view` argument, with its running configuration. You can specify multiple devices with the `-device` argument by separating each device name with a comma or with the `-input` argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of `cwcli config`(1).

start2run

Name	`cwcli config start2run` – CiscoWorks `cwcli config start2run` function
Syntax	`cwcli config start2run -u` *userid* `-p` *password* [`-d` *debuglevel*] [`-m` *email*][`-l` *logfile*] { `-device` *list* | `-view` *name* | `-device` *list* `-view` *name* |`-ipaddress` *list* } [`-config` *1|2*] [`-input` *argumentFile*][`-timeout` *seconds*] [`-primary_user` *primary user name*] [`-primary_pass` *Base64 encoded primary password*] [`-enable_pass` *Base64 encoded enable password*] `cwcli config start2run -help`
Description	`start2run` merges the running configuration of any device(s), specified by the `-device` and/or `-view` arguments, with its startup configuration to give a new running configuration. You can specify multiple devices with the `start2run` argument by separating each device name with a comma or with the `-input` argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of `cwcli config`(1).

write2run

Name	**`cwcli config write2run -`** CiscoWorks **`cwcli config write2run`** function
Syntax	**`cwcli config write2run -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*][**`-m`** *email*][**`-l`** *logfile*] { **`-device`** *name* | **`-ipaddress`** *address*} **`-f`** *filename* [**`-config`** *1*|*2*][**`-listonly`**][**`-input`** *argumentFile*][**`-timeout`** *seconds*][**`-primary_user`** *primary user name*][**`-primary_pass`** *Base64 encoded primary password*][**`-enable_pass`** *Base64 encoded enable password*] **`cwcli config write2run -help`**
Description	**`write2run`** compares the latest running configuration for the device in the configuration archive with the configuration in the file specified by the **`-f`** argument to generate a new configuration that is downloaded to the device, so that the end result is that the configuration specified in the file is available on the running configuration of the device. If **`-listonly`** is specified, the difference between the latest running configuration for the device in the configuration archive and the new configuration that is generated is listed on the display, but no configuration is downloaded to the device. To run this command against multiple devices, specify the **`-input`** argument, which takes a file name as an argument. The contents of the file must be similar to those described in the Input List File Format section of **`cwcli config`**(1). **CAVEAT** This command is not 100% reliable in that it may not successfully overwrite the running configuration. This is due to the dependency on the underlying Diff API, which generates the configuration difference to be downloaded to the device to make the running configuration on the device same as the one specified in the file (by the **`-f`** argument).

write2start

Name	**`cwcli config write2start -`** CiscoWorks **`cwcli config write2start`** function
Syntax	**`cwcli config write2start -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*][**`-l`** *logfile*] { **`-device`** *name* **`-f`** *filename* |**`-ipaddress`** *address*} [**`-config`** *1*|*2*][**`-input`** *argumentFile*][**`-timeout`** *seconds*][**`-primary_user`** *primary user name*][**`-primary_pass`** *Base64 encoded primary password*] [**`-enable_pass`** *Base64 encoded enable password*] **`cwcli config write2start -help`**
Description	**`write2start`** erases the contents of the device's startup configuration and then writes the contents of the given file as the device's new startup configuration. If you do not specify a file name, it prints an error message and exits. To run this command against multiple devices, you must specify the **`-input`** argument, which takes a file name as its argument. The contents of the file must be similar to those described in the Input List File Format section of **`cwcli config`**(1).

listversions

Name	**`cwcli config listversions -`** CiscoWorks **`cwcli config listversions`** function
Syntax	**`cwcli config listversions -u`** *userid* **`-p password`** [**`-d`** *debuglevel*] [**`-m`** *email*][**`-l`** *logfile*]{ **`-device`** *name* | **`-view`** *name* | **`-device`** *name* **`-view`** *name* | **`-ipaddress`** *list*} [**`-baseline`**][**`-input`** *argumentFile*] **`cwcli config listversions -help`**
Description	**`Listversions`** (specified by "listversions") lists the different versions of configuration files archived in the archival system. If you use the **`-baseline`** argument, only the names of the Baseline templates are displayed. You can choose a template and use it inline with the **`comparewithbaseline`** and **`compareanddeploy`** commands.

createdeployparamfile

Name	**`cwcli config createdeployparamfile`** - CiscoWorks **`cwcli config createdeployparamfile`** function.
Syntax	**`cwcli config createdeployparamfile -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*][**`-l`** *logfile*][**`-jobid`** *comparewithbaseline jobid*] [**`-baseline`** *baselinefile*] [**`-f`** *parameterfile*] **`cwcli config createdeployparamfile -help`**
Description	**`createdeployparamfile`** creates a parameter file if the Baseline template containing the parameters is specified. You can use the **`-jobid`** argument to specify the job identifier of the previously executed **`comparewithbaseline`** job. You can choose a template with the **`-baseline`** argument and specify the name of the Baseline template for which the parameter file has to be created.

directbaselinedeploy

Name	**`cwcli config directbaselinedeploy`** - CiscoWorks **`cwcli config directbaselinedeploy`** function
Syntax	**`cwcli config directbaselinedeploy -u`** *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*][**`-l`** *logfile*] { **`-baseline`** *baselinefile* } {**`-substitute`** *parameterfile*}[**`-timeout`** *seconds*] [**`-primary_user`** *primary user name*] [**`-primary_pass`** *Base64 encoded primary password*] [**`-enable_pass`** *Base64 encoded enable password*] **`cwcli config directbaselinedeploy -help`**
Description	**`directbaselinedeploy`** creates a job that downloads the given Baseline template after retrieving the values of the parameters in the template from the given parameter file. You can use the **`-timeout`** argument to specify the duration of the interval in seconds between the two successive polling cycles. You can use the **`-baseline`** to specify the name of the Baseline template which will be compared with the latest configuration version of the device and later downloaded to the device if there are any commands in the baseline config file which are not compliant with the latest configuration of the device in the archive. You can use the **`-substitute`** to substitute the values from the XML parameter file for the parameters specified in the template.

Overview: cwcli netconfig Command

The **`cwcli netconfig`** command lets you use NetConfig from the command line.

Caution The `cwcli netconfig` command does not validate the command arguments you use or the configuration commands that you run using it. If you enter incorrect commands you can misconfigure or disable the devices on which the job runs.

Running the cwcli netconfig Command

To use the `cwcli netconfig` command, you must be able to run the cwcli command, and you must have permissions to use the Adhoc system-defined task. For more details see topic in the section.

The command syntax is:

`cwcli netconfig` *Sub_command Common_arguments Command_arguments*

The subcommands and arguments are described in the following sections:

- Subcommands (see Subcommands)
- Common Arguments (see Common Arguments)
- Command Arguments (see Command Arguments)

Subcommands

Subcommands specify the action the command performs. Valid values for the subcommands are:

Subcommand	Description
createjob	Creates job.
deletejob	Deletes jobs.
canceljob	Cancels jobs.
jobdetails	Lists job details.
jobresults	Lists job results.
listjobs	Lists jobs.
import	Imports user-defined tasks in XML format.
export	Exports user-defined tasks in XML format.
listtasks	Lists the NetConfig user-defined tasks.

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for common_arguments are:

Common Argument	Description	Usage Notes
-u *user*	Enter valid CiscoWorks username.	None
-p *password*	Enter password for username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None

Command Arguments

Command arguments specify parameters that apply only to specific subcommands.

The conventions followed are:

- Arguments in [ ] are optional. For optional arguments, if you do not specify a value the default value that has been set by the administrator using the NetConfig UI, will become applicable.
- Arguments in { } denote that you must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).
- Arguments suffixed with + denote that you can enter multiple values separated with spaces.
- Values that contain spaces need to be entered within " ". For example, the job description that you provide when you use a the **`createjob`** command should be entered within " ".

Valid values for command_arguments are described in the following table:

Sub Command	Command Argument	Description	Usage Notes
`createjob` Allows you to create a NetConfig job.	{**`-device`** *comma_separated_device_names* | **`-devicefile`** *devicelist_filename* | **`-view`** *device_view_name*}	Defines devices to be configured. *comma_separated_device_names* is list of device display names. *devicelist_filename* is path to device list file. Can be full pathname or filename in the local directory. The devicelist file should be of this format: **`-device`** 1.1.1.1,2.2.2.2,3.3.3.3 or **`-device`** 1.1.1.1 **`-device`** 2.2.2.2 **`-device`** 3.3.3.3 *device_view_name* is name of the device view.	Jobs can run only one device category (IOS, Catalyst, Content Engine (CE), or Content Service Switch (CSS)). Do not enter devices of multiple categories.

Sub Command	Command Argument	Description	Usage Notes
	{[{**`-commandfile`** *commandlist_filename* **`-mode`** {`config | enable`}} [**`-rollbackfile`** *rollback_cmdlist_filename*]] [**`-taskname :`** "*User defined task name*"]}	Defines configuration commands to be used. You can specify the command file path, the command mode, the rollback file and the name of the user-defined task. Specify the user-defined task name within quotes.	*commandlist_filename* is path to command file. Can be a full pathname or filename in local directory. **`-mode`** specifies the command mode.{config | enable} are the command mode arguments. By default, **`-mode`** value is set to config. This is not valid for jobs that configure Catalyst devices. For jobs on IOS, CE, or CSS devices, config is default.
			rollback_cmdlist_filename defines the rollback configuration commands for the job. It can be a full pathname to the file or a filename in the local directory. *User defined task name* is the name that you specify for the user-defined task.
	{**`-description :`** *"job_description "*}	Enter the description for the job you are creating.	*"job_description"* is the description you specify, for the job that you are creating. Enter this value within quotes.
	[{**`-schedule`** : *MM/dd/yyyy:HH:mm:ss* **`-schedule_type`**: **`once| weekly| monthly| lastDayOfMonth`**}]	**`-schedule`** defines time and date job will run. If you have enabled Job Approval, and later if you create the job without using the **`-schedule`** argument, the job will automatically be scheduled to run after 5 minutes of the job creation time. You should approve this job within 5 minutes of creating the job. If you want to schedule the job to run at any other time, use the **`-schedule`** argument. If not specified, job will run immediately. **`-schedule_type`** defines the type of job schedule.	*MM* is month (01 to 12). *DD* is day of month (01 to 31). *YYYY* is year (Example: 2004). *HH* is hours, *mm* is minutes, and *ss* is seconds in 24-hour time. If you do not specify the schedule type, the job will be an immediate job.

Sub Command	Command Argument	Description	Usage Notes
	[**`-policyfile`** *policy_filename*]	Defines job policies using a job policy file. You can specify job policies using combination of **`-policyfile`** argument and other optional arguments, However, you can specify each argument only once in command.	*policy_filename* is path to job policy file. Can be a full pathname or filename in local directory.
	[**`-makercomments`** : "*maker comments"*]	Comments from the job creator, to the job approvers, if job approval is enabled for the job.	Enter your comments within quotes.
	[**`-mkemail`** : *maker email id*]	E-mail ID of the job creator, for approval notifications, if approval is enabled for the job.	None
	[**`-execution`**: **`Sequential`**|**`Parallel`**]	Configures the job execution property, whether the jobs should be run sequentially or in parallel.	None.
	[**`-startup`**]: Copy running config to startup policy	Select to cause the configuration job to write the running configuration to the startup configuration on each device after configuration changes are made successfully.	None.
	[**`-version`**] : Fail on mismatch of Config Versions.	Select to cause the job to be considered a failure when the most recent configuration version in the Configuration Archive is not the same as the configuration that was running when you created the job.	**`-sync`** argument should be provided if this policy is selected. This argument causes the job to archive the running configuration before making configuration changes.
	[**`-email`** : *Job Notification email ids*]	Specify the email addresses to which the configuration job will send status notices.	Separate multiple addresses with commas.
	[**`-sync`**] : Synch configuration archive before deploy	Select to cause the job to archive the running configuration before making configuration changes.	None.
	[**`-failure`**: "**`Stop on failure" | "Ignore failure and continue" | "Rollback device and stop" | "Rollback device and continue" | "Rollback job on failure"`**]	Select what the job should do if it fails to run on a device.	Ensure that you place your selected value within quotes.
	[{**`-primary_user`** : *Primary User name* **`-primary_pass`** : "*Primary password"* }]	Primary username for connecting to the device. Primary password for connecting to the device.	Enter the primary password within quotes.

Sub Command	Command Argument	Description	Usage Notes
	[**`-enable_pass`** : "*Execution mode Password"* }]	Password for running commands in the execution mode, on the device.	Enter the execution mode password within quotes.
`deletejob` This subcommand allows you to delete one or more NetConfig jobs.	**`-id`** *job_id*+		*job_id*+ specifies the ID of the job on which to act. You can specify multiple job IDs separated by spaces or commas.
canceljob This subcommand allows you to cancel a NetConfig job from the command line.	**`-id`** *job_id*		*job_id* specifies ID of job on which to act.
jobdetails Allows you to view details of one or more NetConfig jobs from the command line.	[**`-id`** *job_id*+]	Specifies ID of job on which to act.	You can specify multiple job ID separated by spaces or commas.
jobresults Allows you to view results of one or more NetConfig jobs from the command line.	[**`-id`** *job_id*+]	Specifies ID of job on which to act.	You can specify multiple job ID separated by spaces or commas.
	[**`-details`**]	Specifies full details of job results to be displayed.	Not specifying details will display only the summary of job execution result.
`listjobs` Allows you to list all NetConfig jobs from the command line.	[**`-status {A(ll) | R(unning) | C(ompleted) | P(ending)`** }]	Specifies status of jobs to list.	If status is not specified, all registered jobs are listed.
import Allows you to import user defined task in xml format to to netconfig from the command line.	{ **`-taskfile`** *User-defined task file* }	User-defined task filename in XML format.	

Sub Command	Command Argument	Description	Usage Notes
`export` Allows you to export one or more user defined tasks created in netconfig to xml files from the command line.	{ `-task+` *User-defined task name* }	Name of the user-defined task to be exported.	You can specify multiple tasks separated by spaces or commas.
	{`-dest` *file export location* }	Path of the destination location to which the exported user-defined task file is to be copied.	
`listtask`		Lists the NetConfig user-defined tasks.	

Command Examples

Example 1

The command

`cwcli netconfig -u` *username* **`-p`** *password* **`createjob -devicelist`** *device1, device2, device3* **`-commandfile`** *command.file* **`-failure`** *Ignore failure and Continue* **`-startup`**

creates a NetConfig job with the following characteristics:

- Devices *device1, device2, device3* will be configured.
- Commands in file command.file will run.
- Job will continue if it fails to successfully configure a device.
- Each device's running configuration will be copied to startup as soon as the device is successfully configured.
- Job will run immediately because the `-schedule` argument is not specified.

Example 2

The command

`cwcli netconfig -u` *username* **`-p`** *password* **`createjob -devicefile`** *device.file* **`-commandfile`** *command.file* **`-policyfile`** *policy.file*

creates a NetConfig job with the following characteristics:

- Devices listed in the file device.file will be configured.
- Commands in the file command.file will run.
- The file policy.file contains job policy arguments that determine the job policy.

Understanding cwcli netconfig Input Files

Several types of text files are available for you to use as input for the `cwcli netconfig` command and the `-createjob` subcommand. You can also use the command list type as input for user-defined tasks.

File Type	Description	Usage Notes
Device list	Lists devices on which job will run. It lists one device on each line.	Use with **`-devicefile`** argument. Job can run only one device category (IOS, or Catalyst). Do not list devices of multiple categories.
Command list	Lists configuration commands that job will run; one command per line.	Use with **`-commandfile`** argument, or to add commands to a user-defined task.
Job policy	Lists of job policy arguments; one argument per line.	Use with **`-policyfile`** argument.

Examples

Device List File

```
devicename1
devicename2
devicename3
devicename4
```

Command List File

```
command1
command2
command3
command4
```

Job Policy File

This file configures the job to stop running if the job fails on a device, to write the running configuration to startup after configuration changes are made.

```
-failure Stop on Failure
-sync
```

cwcli netconfig Man Page Examples

On UNIX, you can view the complete man pages by setting the MANPATH to /opt/CSCOpx/man

The following are some examples from the NetConfig man page:

Examples

Device List File Example

For the command

cwcli netconfig createjob -u *userid* **-p** *password* **-devicefile** *c7000.dev* **-commandfile** *command.file*

-description *"cwcli netconfig job"* **-mode** `config`

An example of the device list file c7000.dev is

```
enm-7000-1.cisco.com

enm-7000-2.cisco.com
```

```
enm-7000-3.cisco.com

enm-7000-4.cisco.com
```

Command List File Example

For the command

`cwcli netconfig createjob -u` *userid* **`-p`** *password* **`-devicelist`** *c7000-1,c7000-2* **`-commandfile`** *command.file*

`-description` *"cwcli netconfig job"* **`-mode`** `config`

An example of the command file command.file is

```
snmp-server community public ro

snmp-server community private rw
```

Policy File Example

For the command

`cwcli netconfig createjob -u` *userid* **`-p`** *password* **`-devicefile`** *c7000.dev* **`-commandfile`** *command.file* **`-policyfile`** *policy.in*

`-description` *"cwcli netconfig job"* **`-mode`** `config`

An example of the policy file policy.in is

`-failure` *"Stop on failure"*

`-sync`

`-execution` `Parallel`

User-defined Task XML file Example

```
<?xml version="1.0" encoding="UTF-8"?>

<Task name="SampleTASK">

<Template mode="1" name="iproute" parameterized="false">

<Commands>

<cli>ip route 0.0.0.1 0.0.0.0 Ethernet0/0</cli>

<cli>ip route 0.0.0.2 0.0.0.0 Ethernet0/0</cli>

<cli>ip route 0.0.0.3 0.0.0.0 Ethernet0/0</cli>

<cli>ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>

<cli>ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>

<cli>ip route 0.0.0.6 0.0.0.0 Ethernet0/0</cli>

</Commands>

<RollbackCommands>

<cli>no ip route 0.0.0.4 0.0.0.0 Ethernet0/0</cli>

<cli>no ip route 0.0.0.5 0.0.0.0 Ethernet0/0</cli>

</RollbackCommands>

<MDFIds>268438030,273153536,272819655</MDFIds>

</Template>
```

```
</Task>
```

cwcli netconfig Remote Access

You can also perform the **`cwcli netconfig`** tasks using the servlet. You will have to upload a payload XML file, which contains the **`cwcli netconfig`** command arguments and CiscoWorks user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

`perl` *samplepost.pl* **`http://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`perl` *samplepost.pl* **`https://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>

<command>

cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...

</command>

</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

`http://<rme-server>:<rme-port>/rme/cwcli?command=cwcli netconfig` *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`https://`*rme-server:rme-port***`/rme/cwcli?command=cwcli netconfig`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Overview: cwcli export Command

`cwcli export` is a command line tool that also provides servlet access to inventory, configuration and change audit data.

This can be used for generating inventory, configuration archive, and change audit data for devices in Resource Manager Essentials (RME).

Note You cannot run this command for the RME devices that are in Conflicting or Suspended state.

This tool supports the following features:

- Generating change audit data in XML format

  The tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.

  See Running cwcli export changeaudit for the usage and XML schema details
- Generating configuration data in XML format

  The tool uses existing configuration archive APIs and generates latest configuration data from the configuration archive in XML format.

  Elements in the XML file are created at the configlet level in the current configuration archive. Predefined rules that currently exist in the configuration archive are used to get the configlets data.

  See Running cwcli export config for the usage and XML schema details
- Generating inventory data in XML format

  The tool has servlet access and command line utilities that can generate inventory data for devices managed by the RME server.

  See Running cwcli export inventory Command for the usage and XML schema details

The `cwcli export` command is located in the following directories, where *install_dir* is the directory in which CiscoWorks is installed:

- On UNIX systems, /opt/CSCOpx/bin
- On Windows systems, *install_dir*\CSCOpx\bin

  The default install directory is C:\Program Files.

If you install RME on an NTFS partition on Windows, only users in the administrator or casuser group can access `cwcli export`. Users with read-execute access to the CSCOpx\files\archive directory and the directories under that can also use `cwcli export`.

You can also perform the `cwcli export` tasks using the servlet. You will have to upload a payload XML file, which contains the `cwcli export` command arguments and CiscoWorks user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

perl *samplepost.pl* **http://***rme-server:rme-port***/rme/cwcli** *payload_XML_file*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`perl` *samplepost.pl* **`https://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>

<command>

cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...

</command>

</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

`http://`*rme-server:rme-port***`/rme/cwcli?command=cwcli export`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`https://`*rme-server:rme-port***`/rme/cwcli?command=cwcli export`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Using the cwcli export Command

The command line syntax of the application is in the following format:

`cwcli export` *command GlobalArguments AppSpecificArguments*

- **`cwcli export`** is the CiscoWorks command line interface for exporting inventory/config/changeaudit details into XML format.
- *Command* specifies which core operation is to be performed.
- *GlobalArguments* are the additional parameters required for each core command.
- *AppSpecificArguments* are the optional parameters, which modify the behavior of the specific **`cwcli export`** core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after **`cwcli export`**.

The following sections describe:

- The **`cwcli export`** commands (See cwcli export Commands)

- The mandatory and optional arguments (See cwcli export Global Arguments)
- The default archiving location (See Archiving cwcli export Data in XML File)

On UNIX, you can view the `cwcli export` man pages by setting the MANPATH to /opt/CSCOpx/man.

The commands to launch the `cwcli export` man pages are:

- `man cwcli-export`—To launch the `cwcli export` command man page.
- `man export-changeaudit`—To launch the `cwcli export changeaudit` command man page.
- `man export-config`—To launch the `cwcli export config` command man page.
- `man export-inventory`—To launch the `cwcli export inventory` command man page.

cwcli export Commands

The following table lists the command part of the `cwcli export` syntax.

Command	Description
`cwcli export changeaudit`	Generates Change Audit log data in XML format.
`cwcli export config`	Generates configlets in XML format
`cwcli export inventory`	Generates Inventory data in XML format.

You must invoke the `cwcli export` command with one of the core commands specified in the above table. If no core command is specified, `cwcli export` can execute the `-v` or `-h`. arguments only. Argument `-v` specifies the version of the `cwcli export` utility and argument `-h` (or null argument) displays the usage information of this tool.

cwcli export Global Arguments

The following describes the mandatory and optional global arguments for `cwcli export`:

Global Arguments	Description
-u *userid*	Mandatory Specifies the CiscoWorks username.

Global Arguments	Description
`-p` *password*	Mandatory Specifies the password for the CiscoWorks username. If you want to avoid the **`-p`** argument which will reveal the password in clear text in cli, you will have to store your username and password in a file and set a variable `cwcli` *`CWCLIFILE`* which points to the file. You will have to maintain this file and control access permissions to prevent unauthorized access. **`cwcli export`** looks for current working directory if `cwcli` *`CWCLIFILE`*is set only to file name instead of full path. If you use the **-p** argument, even after setting the `cwcli` *`CWCLIFILE`* variable the password is taken from the command line instead of `cwcli` *`CWCLIFILE`*. This is not secure and usage of this argument is not recommended. The password must be provided in the file in the following format: username password where username is the CiscoWorks user name given in the command line.The delimiter between the username and password is single blank space. You must enter the delimiter if the password is blank. Otherwise, **`cwcli export`** will fail to validate the password.The password file can contain multiple entries with different user names. The password that matches first is considered in case of duplicate entries. **Note** If **`-p`** *password* is used, the password is read from the command line instead of `cwcli` *`CWCLIFILE`*. This is highly insecure and therefore not recommended. See Setting CWCLIFILE Environment Variable for more details.
{ **`-device`** *devicename* | **`-view`** *viewname*| **`-input`** *inputfilename* | **`-ipaddress`** *mgmt-ip-address* }	Mandatory **`-device`** *devicename* Specifies the display name of the device that you have added in the Device and Credentials database (Common Services > Device and Credentials > Device Management). You can enter multiple display name separated by a comma. You can use either wildcard or specific device(s) but not at the same time. The argument syntax used for **`-device`** argument may be a single device or a device list. Devices in a list are separated by a ','. The wild card symbol '**%**' may be used to specify a group of devices having a pattern. For example if a pattern ***x%*** is specified as a device in the list, then all the CiscoWorks devices that have names that start with x will be selected for this operation.
{ **`-device`** *devicename* | **`-view`** *viewname* | **`-input`** *inputfilename* | **`-ipaddress`** *mgmt-ip-address*}	Mandatory **`-view`** *viewname* If the data needs to be generated for all the devices in a specific group, you can use the **`-view`** argument. You can use this argument to generate data for devices in all RME device views including system-defined groups and user-defined groups. You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration window. To separate the path you must use forward slash only. For example, **`-view`** "/RME@*ciscoworks_servername*/All Devices"

Global Arguments	Description
{ **`-device`** *devicename* | **`-view`** *viewname* **`-input`** *inputfilename* | **`-ipaddress`** *mgmt-ip-address*}	Mandatory **`-input`** *inputfilename* You can create an input list file that contains a list of devices to perform the operation on. The contents of the input list file are a sequence of lines. Each line specifies a display name as entered in the Device and Credential Repository. The arguments must be specific to the function. You cannot include group names in the input list file. You can include comments in the input list file by starting each commented line with #. The input file should be of this format: **`-device`** 1.1.1.1,2.2.2.2,3.3.3.3 or **`-device`** 1.1.1.1 **`-device`** 2.2.2.2 **`-device`** 3.3.3.3
{ **`-device`** *devicename* | **`-view`** *viewname* **`-input`** *inputfilename* | **`-ipaddress`** *mgmt-ip-address*}	Mandatory **`-ipaddress`** *mgmt-ip-address* Specify the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with **`-device`**, **`-view`**, or **`-input`**. Also, you cannot specify wildcard characters.
`-d` *debuglevel*	Optional *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.
`-l` *logfile*	Optional Logs the results of the **`cwcli export`** command to the specified log file name. By default the command output will be displayed on the standard out.
`-m` mailid	Optional Mails the results of the **`cwcli export`** command to the specified email address. This argument notifies you whether the task is completed. Only one mail id can be given at a time.
`-f` *filename*	This is applicable only for changeaudit and inventory applications. Optional Specifies the name of the file to which the changeaudit and inventory information is to be exported on CiscoWorks server. If you are using **`cwcli`** remotely (get or post request), by default the output file is available at this location on CiscoWorks server: On Windows: *NMSROOT*\MDC\tomcat Where, *NMSROOT* is the CiscoWorks installed directory. On Solaris: /opt/CSCOpx/objects/dmgt

Archiving cwcli export Data in XML File

By default, the data generated through `cwcli export` command is archived at the location:

cwcli export *Command*	**Location on CiscoWorks Server**
changeaudit	On Solaris: /var/adm/CSCOpx/files/rme/archive/*YYYY-MM-DD-HH-MM-SS* -changeaudit.xml
	On Windows: *NMSROOT*\files\rme\archive\YYYY-MM-DD-HH-MM-SS -changeaudit.xml
config	On Solaris: /var/adm/CSCOpx/files/rme/cwconfig/*YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name*.xml
	On Windows: *NMSROOT*\files\rme\cwconfig\*YYYY-MM-DD-HH-MM-SS-MSMSMS -Device_Display_Name*.xml
inventory	On Solaris: /var/adm/CSCOpx/files/rme/archive/*YYYY-MM-DD-HH-MM-SS*-inventory.xml
	On Windows: *NMSROOT*\files\rme\archive\YYYY-MM-DD-HH-MM-SS-inventory.xml

Where *NMSROOT* is the RME installed directory.

You can also specify a directory to store the output. This application does not have a feature to delete the files created in the archive. You should delete the files when necessary.

While generating data through the servlet, the output will be displayed in the client terminal.

Running cwcli export changeaudit

Using this command you can export the Change Audit log data in the XML format.

The command syntax for `cwcli export changeaudit` is:

```
cwcli export changeaudit {-u username -p password -device devicenames}
[- ipaddress mgmt-ip-address]
    [-f filename]
    [-from mm/dd/yyyy] ---> eg: 05/01/2004
    [-to mm/dd/yyyy]  ---> eg: 05/06/2004
    [-app comma separated list of applications]
    [-cat comma separated list of categories]
```

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you enter an argument which has space then use double quotes for that argument. For example for Software Management, you enter this as “Software Management”.

The following table describes the arguments that are specific to **`cwcli export changeaudit`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli export Command.

Arguments	Description
[**`-from`** *mm/dd/yyyy*]	Optional. Enter the from date. If you enter only **`-from`** date then the report will be generated from the date that you have specified, to the current date.
[**`-to`** *mm/dd/yyyy*]	Optional. Enter the from date. If you enter only **`-to`** date then the report will be generated from the date RME has logged Change Audit record to the **`-to`** date that you have specified.
[**`-app`** *comma separated list of applications*]	Specify the application name. The supported applications are: • Archive Mgmt • ConfigEditor • CwConfig • ICServer • NetConfig • Software Management If you do not specify the **`-app`** argument, then changes made by all applications is reported.
[**`-cat`** *comma separated list of categories*]	Specify the category name. The supported categories are: • CONFIG_CHANGE—Configuration changes on the device. • INVENTORY_CHANGE—Hardware changes on the device. • SOFTWARE_CHANGE—Software changes on the device. If you do not specify the **`-cat`** argument, then changes made by all categories is reported.

Note If you do not enter **`-from`** and **`-to`** arguments, all the Change Audit records logged till the current date will be displayed.

The following sections describes:

- XML Schema for cwcli export changeaudit
- XML Schema for Configuration Management Application
- XML Schema for Software Management
- Usage Examples for cwcli export changeaudit Command

XML Schema for cwcli export changeaudit

The following is the schema used for exporting the change audit data in XML format.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c http://www.w3.org/2000/10/XMLSchema-->
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">
 <xsd:element name = "changeRecord">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "groupId"/>
    <xsd:element ref = "category"/>
    <xsd:element ref = "host"/>
    <xsd:element ref = "user"/>
    <xsd:element ref = "device"/>
    <xsd:element ref = "connectionMode"/>
    <xsd:element ref = "timestamp"/>
    <xsd:element ref = "description"/>
   </xsd:sequence>
   <xsd:attribute name = "id" use = "required" type = "xsd:integer"/>
  </xsd:complexType>
 </xsd:element>
 <xsd:element name = "groupId" type = "xsd:string"/>
 <xsd:element name = "category" type = "xsd:string"/>
 <xsd:element name = "application" type = "xsd:string"/>
 <xsd:element name = "host" type = "xsd:string"/>
 <xsd:element name = "user" type = "xsd:string"/>
 <xsd:element name = "device" type = "xsd:string"/>
 <xsd:element name = "connectionMode" type = "xsd:string"/>
 <xsd:element name = "timestamp" type = "xsd:string"/>
 <xsd:element name = "description">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "summary"/>
    <xsd:element ref = "details"/>
   </xsd:sequence>
  </xsd:complexType>
 </xsd:element>
 <xsd:element name = "summary" type = "xsd:string"/>
 <xsd:element name = "details">
  <xsd:complexType/>
 </xsd:element>
 <xsd:element name = "changeRecordSet">
  <xsd:complexType>
   <xsd:sequence>
    <xsd:element ref = "changeRecord" maxOccurs = "unbounded"/>
   </xsd:sequence>
  </xsd:complexType>
 </xsd:element>
</xsd:schema>
```

Detailed Description of changeaudit Schema

The table below describes elements in the changeaudit schema:

Field	Description
Category	Type of the change. For example, configuration, inventory, or software.
Application	Name of the RME application involved in the network change (Device Configuration, Inventory, or Software Management).
Host	Host device from which the user accessed the device or the host name of the RME server.

Field	Description
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the RME application is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or RME application.
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Description	Contains the detailed information of the changes that had occurred on the device. The description changes based on the application you have selected: • Archive Mgmt (See XML Schema for Configuration Management Application for more information.) • ConfigEditor (See XML Schema for Configuration Management Application for more information.) • CwConfig (See XML Schema for Configuration Management Application for more information.) • ICServer—Inventory Collection Service (See XML Schema for Inventory Collection Service for more information.) • NetConfig (See XML Schema for Configuration Management Application for more information.) • Software Management (See XML Schema for Software Management for more information.)

The following section describes the schema used by these application when you run the command **`cwcli export changeaudit`** with **`-app`** argument:

- Archive Mgmt, ConfigEditor, CwConfig, NetConfig
- Inventory Collection Service
- Software Management

XML Schema for Configuration Management Application

The following XML schema is used by all Configuration Management application when you run the **`cwcli export changeaudit`** command with **`-app`** argument and the **`-app`** argument values as either *Archive Mgmt*, *ConfigEditor*, *CwConfig*, or *NetConfig*.

The schema file is:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--  edited with XMLSPY v2004 rel. 2 U (http://www.xmlspy.com) by Cisco (t) -->
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    - <xs:element name="ConfigDiff">
        - <xs:annotation>
            <xs:documentation>Comment describing your root element</xs:documentation>
          </xs:annotation>
        - <xs:complexType>
            - <xs:sequence>
            - <xs:element name="OldConfig">
                - <xs:complexType>
                    - <xs:sequence>
                        <xs:element name="Command" maxOccurs="unbounded" />
                      </xs:sequence>
                      <xs:attribute name="Version" type="xs:integer" />
                  </xs:complexType>
              </xs:element>
    - <xs:element name="NewConfig">
        - <xs:complexType>
            - <xs:sequence>
                <xs:element name="Command" maxOccurs="unbounded" />
            </xs:sequence>
                      <xs:attribute name="Vesrion" type="xs:integer" />
                  </xs:complexType>
              </xs:element>
          </xs:sequence>
          <xs:attribute name="CASLogID" type="xs:integer" />
          <xs:attribute name="DeviceName" type="xs:string" />
      </xs:complexType>
  </xs:element>
</xs:schema>
```

Detailed Description of Configuration Management Schema

The table below describes elements in the Configuration Management schema.

Field	**Description**
Category	Type of the change. For example, configuration, inventory, or software.
Host	Host device from which the user accessed the device or the host name of the RME server.
Application	Name of the application. For example, Archive Mgmt, NetConfig, etc.
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the RME application is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or RME application.
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.

Field	Description
Summary	Description describing what caused the change. For example: • Configuration Download due to job • Syslog triggered Config Collection
ConfigDiff	• FirstConfig, SecondConfig • DeviceName—Network device on which the change occurred. The display name as entered in the Device and Credential Repository. • Version—Configuration file version number. • CommandDiff Polarity—Changes in the configuration file. – POSNEG—No change – POSITIVE —Added new commands – IGNORED—Ignored the commands – NEGATIVE—Deleted the commands

XML Schema for Inventory Collection Service

The following XML schema is used by Inventory Collection Service application when you run the **`cwcli export changeaudit`** command with **`-app`** argument and the **`-app`** argument values as ICServer.

The schema file is:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<xsd:schema xmlns:xsd = "http://www.w3.org/2000/10/XMLSchema">
<xsd:element name = "InventoryChangeDetailRecord">
    <xsd:complexType>
        <xsd:sequence maxOccurs = "unbounded">
            <xsd:element ref = "Section"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name = "Section">
    <xsd:complexType>
        <xsd:sequence maxOccurs = "unbounded">
            <xsd:element ref = "Attributes"/>
        </xsd:sequence>
        <xsd:attribute name = "Name" type = "xsd:string"/>
        <xsd:attribute name = "Identity" type = "xsd:string"/>
    </xsd:complexType>
</xsd:element>
<xsd:element name = "Attributes">
    <xsd:complexType>
        <xsd:all maxOccurs = "unbounded">
            <xsd:element ref = "Previous_value"/>
            <xsd:element ref = "Current_value"/>
            <xsd:element ref = "Action"/>
        </xsd:all>
    </xsd:complexType>
</xsd:element>
    <xsd:element name = "Previous_value" type = "xsd:string"/>
    <xsd:element name = "Current_value" type = "xsd:string"/>
    <xsd:element name = "Action" type = "xsd:string"/>
</xsd:schema>
```

Detailed Description of Inventory Collection Service Schema

The table below describes elements in the Inventory Collection Service schema.

Field	Description
Name	Name of the physical and logical entities. The main physical entities are Chassis, Backplane, Card, CommunicationConnector, FlashDevice, FlashPartition, FlashFile, SoftwareIdentity, PhysicalMemory The main logical entities are ManagedNetworkElement, LogicalModule, Port, MemoryPool, OSElement, IPProtocolEndpoint, IfEntry, AdditionalInformation See Detailed Description of the Inventory Schema for further information.
Identity	Identifies the entity that has changed on the device. For example: If the Flash File name has changed then Identity will be Flash Device 2, Flash Partition 3.
AttributeName	Name of the different physical and logical entities For example: In MemoryPool, the different entities are User, Free, PoolType. See Detailed Description of the Inventory Schema for further information.
Previous_value	Value of the entity before the change occurred.
Current_value	Value of the entity after the change occurred.
Action	Type of change that has occurred on the device: • Inserted— Added a new entity. • Changed—Changed in the entity. • Deleted—Deleted an entity.

XML Schema for Software Management

The following XML schema is used by Software Management application when you run the **`cwcli export changeaudit`** command with **-app** argument and the **-app** argument values as Software Management.

The schema file is:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--  edited with XMLSPY v2004 rel. 2 U (http://www.xmlspy.com) by Cisco -->
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
- <xs:element name="SwimHistoryRecord">
   - <xs:annotation>
      <xs:documentation>Models a set of image changes on the device.</xs:documentation>
   </xs:annotation>
- <xs:complexType>
   - <xs:sequence>
      - <xs:element name="JobID" type="xs:positiveInteger" minOccurs="0">
   - <xs:annotation>
      <xs:documentation>ID of the Job in which the change happened</xs:documentation>
   </xs:annotation>
   </xs:element>
   - <xs:element name="ImageChange" maxOccurs="unbounded">
- <xs:complexType>
   - <xs:sequence>
```

```
          <xs:element name="OldImage" type="Image" />
          <xs:element name="NewImage" type="Image" />
      </xs:sequence>
      <xs:attribute name="ID" type="xs:positiveInteger" use="required" />
      </xs:complexType>
      </xs:element>
      </xs:sequence>
  </xs:complexType>
</xs:element>
- <xs:complexType name="Image">
- <xs:annotation>
     <xs:documentation>Models an Image.</xs:documentation>
  </xs:annotation>
- <xs:sequence>
    - <xs:element name="Type">
        - <xs:annotation>
          <xs:documentation>Label of corresponding image type from enumeration
        com.cisco.nm.xms.xdi.ags.imageparser.ImageType</xs:documentation>
          </xs:annotation>
        - <xs:simpleType>
            - <xs:restriction base="xs:string">
            <xs:whiteSpace value="preserve" />
          </xs:restriction>
        </xs:simpleType>
        </xs:element>
      <xs:element name="Name" type="xs:string" />
      <xs:element name="Version" type="xs:string" />
- <xs:element name="Attribute" minOccurs="0" maxOccurs="unbounded">
    - <xs:complexType>
    - <xs:sequence>
        - <xs:element name="AttributeName">
        - <xs:simpleType>
            - <xs:restriction base="xs:string">
            <xs:whiteSpace value="preserve" />
      </xs:restriction>
      </xs:simpleType>
  </xs:element>
- <xs:element name="AttributeValue">
    - <xs:simpleType>
        - <xs:restriction base="xs:string">
         <xs:whiteSpace value="preserve" />
      </xs:restriction>
      </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

Detailed Description of Software Management Schema

The table below describes elements in the Software Management schema.

Field	Description
Category	Type of the change. For example, configuration, inventory, or software.
Host	Host device from which the user accessed the device or the host name of the RME server.

Field	Description
Application	Name of the application. For example, Archive Mgmt, NetConfig, etc.
User	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the RME application is running, or the name under which the Telnet connection is established.
Device	Network device on which the change occurred. The display name as entered in the Device and Credential Repository.
ConnectionMode	Connection mode through which the change was made, for example, Telnet, snmp, console, or RME application.
Timestamp	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Summary	Description describing what caused the change. For example, Software upgrade.
Job ID	Job ID for the Software Upgrade.
OldImage	Displays the details on device type, name of the software image, and version of the image.
NewImage	Displays the details on device type, name of the software image, and version of the image.

Usage Examples for cwcli export changeaudit Command

This section provides some examples of usage for the **`cwcli export changeaudit`** command.

Example 1: To generate the Change Audit report for all applications and categories for a particular RME device group.

`cwcli export changeaudit -u` *admin* **`-p`** *admin* **`-view`** *"/RME@ciscoworksservername/Normal Devices"*

```
SUMMARY

========

        Successful: export:
D:/PROGRA~1/CSCOpx/files/rme/archive/2004-10-15-04-09-42-changeaudit.xml
```

Example 2: To generate the Change Audit report for a specific application and category for a device in a given time frame

`cwcli export changeaudit -u` *admin* **`-p`** *admin* **`-device`** *10.6.8.6* **`-from`** *09/30/2004* **`-to`** *10/15/2004* **`-app`** "*Archive Mgmt*" **`-cat`** *CONFIG_CHANGE*

```
SUMMARY

========

        Successful: export:
D:/PROGRA~1/CSCOpx/files/rme/archive/2004-10-15-04-44-50-changeaudit.xml
```

Example 3: To generate the Change Audit report in the given output file

`cwcli export changeaudit -u` *admin* **`-p`** *admin* **`-device`** % **`-f`** *changeaudit.xml*

```
SUMMARY

========

        Successful: export: changeaudit.xml
```

The output for this is written to the changeaudit.xml file in the *Install_dir*/CSCOpx/bin directory. Where *Install_dir* is the CiscoWorks installed directory.

Example 4: To generate the Change Audit using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for “%”
- %2f is the URL encode for “_”

Enter this in your browser:

http://*ciscowork_servername***:1741/rme/cwcli?command=cwcli export changeaudit -u** *admin* **-p** *YWRtaW4=* **-device** *10.7.3.8* **-app** *%22Archive Mgmt%22* **-cat** *%22CONFIG%2fCHANGE%22* **-f** *changeaudit.xml*

The output for this is written to the changeaudit.xml file.The changeaudit.xml file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the CiscoWorks installed directory.

On Solaris:

/opt/CSCOpx/objects/dmgt

Example 5: To generate the Change Audit report using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *changeaudit.xml* contains:

```
<payload>

   <command>

cwcli export changeaudit -u admin -p YWRtaW4= -device 1.6.8.6 -from 09/30/2004 -app
"Archive Mgmt" -cat CONFIG_CHANGE -view "/RME@CiscoWorks_servername/Pre-deployed" -f
changeauditreport.xml

   </command>

</payload>
```

At the command prompt enter:

perl *samplepost.pl* **https://CiscoWorks_Servername:443/rme/cwcli** *changeaudit.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
SUMMARY

========

        Successful: export: changeauditreport.xml

<!-- Processing complete -->
```

The output for this is written to the *changeauditreport.xml* file.The *changeauditreport.xml* file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the CiscoWorks installed directory.

On Solaris:

/opt/CSCOpx/objects/dmgt

Running cwcli export config

Using this command you can retrieve the configuration data in the XML format specified by the schema. The Configlet Generator provides a wrapper over the existing Config Archive to retrieve configlets data for the selected device. The exported data contains the entire running configuration data.

The command syntax for **`cwcli export config`** is:

`cwcli export config`{**`-u`** *username* **`-p`** *password*} [**`-d`** *debuglevel*] [**`-m`** *mailid*] [**`-l`** *logfile*] {**`-device`** *devicename* | **`-input`** *inputfilename* | **`-view`** *viewname* | **`- ipaddress`** *mgmt-ip-address*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you enter an argument which has space then use double quotes for that argument.

The following table describes the argument that is specific to **`cwcli export config`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli export Command.

Arguments	Description
`-s 1`	Optional. Displays the exported configuration file on the console. If you use this command, you can specify only one device. You cannot export the configuration files of multiple devices. To export the configuration files of multiple devices, either make multiple requests to the servlet, or get these files from the CiscoWorks server. Usage of this option: **`cwcli export config -u`** *admin* **`-p`** *admin* **`-device`** 10.22.33.44 **`-s 1`**

The output files depends on the number of devices specified. There are as many configuration XML output files as the number of devices. The output files are created under this location on CiscoWorks server:

On Solaris:
/var/adm/CSCOpx/files/rme/cwconfig/*YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml*

On Windows:
NMSROOT\files\rme\cwconfig\YYYY-MM-DD-HH-MM-SS-XXX-Device_Display_Name.xml

Where *NMSROOT* is the CiscoWorks installed directory.

XML Schema for cwcli export config

The following is the schema used for exporting the configuration data in XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 4 U (http://www.xmlspy.com) by Cisco -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="DeviceConfiguration">
<xs:annotation>
<xs:documentation>This has list of Configlets</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:sequence>
<xs:element ref="Confilglet" maxOccurs="unbounded"/>
<xs:element name="DeviceName" type="xs:string">
<xs:annotation>
<xs:documentation>Device Name as managed by RME</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="DeviceFamily" type="xs:string">
<xs:annotation>
<xs:documentation>MDF devcie family</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="CreationTime" type="xs:date">
<xs:annotation>
<xs:documentation>Date and Time this was created</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="Version" type="xs:string">
<xs:annotation>
<xs:documentation>Config File Version</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="Data" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Confilglet">
<xs:annotation>
<xs:documentation>Configlet can have subconfiglets</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:sequence>
<xs:element ref="Confilglet" minOccurs="0" maxOccurs="unbounded"/>
<xs:element name="command" minOccurs="0" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:string">
<xs:attribute name="LineNo"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="SubModeCommand" type="xs:string" minOccurs="0">
<xs:annotation>
<xs:documentation>Command to change the mode</xs:documentation>
</xs:annotation>
</xs:element>
</xs:sequence>
<xs:attribute name="Name" type="xs:string" use="required">
<xs:annotation>
<xs:documentation>Configlet Name</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Checkedout" type="xs:boolean" use="optional" default="false">
<xs:annotation>
```

```
<xs:documentation>Future Use </xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Rebuild" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specifies if the entire list of commands in particular configlet needs a rebuild if any of
the coammnds is modified</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Submode" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specfies if the commands under the configlet falls under a submode</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="OrderSensitive" type="xs:boolean" use="optional" default="false">
<xs:annotation>
<xs:documentation>Specifies if the commands in the configlet are oreder sensitive or not</xs:documentation>
</xs:annotation>
</xs:attribute>
</xs:complexType>
</xs:element>
</xs:schema>
```

Detailed Description of config Schema

The table below describes elements in the config schema:

Field	Description
Device	Device display name as entered in the Device and Credential Repository.
Date	Date and time at which the configuration changes have occurred.
Version	Configuration file version.
Configlet name	Name of the configlet. The available configlets vary from device to device; the following are examples: • SNMP displays SNMP configuration commands, for example, snmp-server community public RO. • IP Routing displays IP routing configuration commands, for example, router abcd 100. • Interface folder displays the different interface configuration commands, for example, Interface Ethernet0 and Interface TokenRing. • Global displays global configuration commands, for example no ip address. • Line con 0 displays configuration commands for line console 0. • IP displays IP configuration commands, for example, ip http server.

Usage Examples for cwcli export config Command

This section provides some examples of usage for the **`cwcli export config`** command.

Example 1: To generate the config report for a particular RME device group

`cwcli export config -u` *admin* **`-p`** *admin* **`-view`** *"/RME@ciscoworksservername/Normal Devices"*

```
SUMMARY

========
        Successful: ConfigExport:D:/PROGRA~1/CSCOpx/files/rme/cwconfig
```

The output folder will contain separate config file for every devices in the Normal Devices group.

Example 2: To generate the config report for the devices that are specified in the device input file

The input configdevices.txt contains these devices:

`-device` 10.22.33.44,10.22.33.55,1.1.1.1

`cwcli export config -u` *admin* **`-p`** *admin* **`-input`** *configdevices.txt*

Example 3: To generate the config using the cwcli get request

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for "%"

Enter this in your browser:

`http://`*ciscowork_servername***`:1741/rme/cwcli?command=cwcli export config -u`** *admin* **`-p`** *YWRtaW4=* **`-device`** *%25*

```
<!-- Processing Starts  -->

SUMMARY

========

Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig

<!-- Processing complete -->
```

Example 4: To generate the Change Audit report using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *config.xml* contains:

```
<payload>

   <command>

cwcli export config -u admin -p YWRtaW4= -device 1.6.8.6

   </command>

</payload>
```

At the command prompt enter:

`perl` *samplepost.pl* **`https://CiscoWorks_Servername:443/rme/cwcli`** *config.xml*

```
<!-- Processing Starts  -->


SUMMARY

========

        Successful: ConfigExport: D:/PROGRA~1/CSCOpx/files/rme/cwconfig

<!-- Processing complete -->
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

Running cwcli export inventory Command

Using this command you can export inventory data in the XML format.

The command syntax for **`cwcli export inventory`** is:

`cwcli export inventory` {**`-u`** *username* **`-p`** *password*}[**`-d`** *debuglevel*] [**`-m`** *mailid*] [-l *logfile*] [**`-f`** *filename*] {**`-device`** *devicename* | **`-input`** *inputfilename* | **`-view`** *viewname* | **`- ipaddress`** *mgmt-ip-address*} [**`-hop`** *hopdevice*]

The above command retrieves the inventory data in XML format specified by the schema. The **`-f`** parameter stores the output in the file specified by *filename*. If you have not specified the filename, the output is stored at the following location:

PX_DATADIR/rme/archive/timestampinventory.xml

Where *PX_DATADIR* is the *NMSROOT*/files directory and *NMSROOT* is the RME installed directory.

The device name can also have a wild card symbol "**%**" to choose all devices with that particular name.

If the number of devices is large, the list of devices can be stored in an input file and the name of the input file can be given in the command line.The input argument cannot occur with the device or view arguments.

If the data needs to be generated for all the devices in a specific group, you can use the **`-view`** argument. You can use this argument to generate data for devices in all RME device groups including system-defined groups and user-defined groups.

The following table describes the arguments that are specific to **`cwcli export inventory`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli export Command.

Arguments	Description
`-hop` *hopdevice*	Optional Used to increase performance by using more memory. This indicates the number of devices to be worked upon at a time. By default, this value is 1.

Given below is the list of combinations, which could occur for the inventory command.

`cwcli export inventory -u` *admin* **`-p`** *admin* **`-f`** *myinv.xml*

`cwcli export inventory -u` *admin* **`-p`** *admin* **-f** *myinv.xml* **`-device`** *device1*

`cwcli export inventory -u` *admin* **`-p`** *admin* **`-device`** *device%*

`cwcli export inventory -u` *admin* **`-p`** *admin* **`-input`** *inv.txt*

`cwcli export inventory -u` *admin* **`-p`** *admin* **`-view`** *"/RME@ciscoworksservername/Normal Devices*"

`cwcli export inventory -u` *admin* **`-p`** *admin* **`-f`** *myinv.xml* **`-input`** *inv.txt*

To apply the **`cwcli export`** command on more than one CiscoWorks device you must use the format in the example given below. The parameter, inputlist, is a text file which will have the list of device names separated by a new line. A line starting with # will be treated as a comment.

Example:

```
#comment
```

```
-device device1,device2,device3
```

```
#comment
```

where device1, device2, and device3 are device displaynames.

XML Schema for cwcli export inventory Data

The following is the schema used for exporting the inventory data in XML format.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<xs:schema xmlns:xs = "http://www.w3.org/2001/XMLSchema" elementFormDefault = "qualified"
attributeFormDefault = "unqualified">
        <!--This schema is based on the classes defined in Cisco Information Model V2.0 (CIMCXV2.0)
Each Device has Chassis and NetworkElement.
Chassis:
        Chassis contains a blackplane and multiple Cards. Each Card contains CommunicationConnectors and
multiple daughter cards. Flash Devices reside on the Cards.
NetworkElement:
System Information, Interface Information and LogicalModules. LogicalModules contain OSElements and Logical
Ports.
The element AdditionalInformation is meant to capture device specific details that are not part of the common
schema.
-->
<xs:element name = "InvDetails">
<xs:complexType>
<xs:sequence>
<xs:element ref = "SchemaInfo" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "RMEPlatform" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "SchemaInfo">
<xs:complexType>
<xs:sequence>
<xs:element name = "RMEServer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "CreatedAt" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SchemaVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "RMEPlatform">
<xs:complexType>
<xs:sequence>
<xs:element ref = "Cisco_Chassis" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_NetworkElement" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_ComputerSystemPackage" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Chassis">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "HardwareVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ChassisSystemType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfSlots" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NoOfCommunicationConnectors" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_Backplane" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Card" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
```

```
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Backplane">
<xs:complexType>
<xs:sequence>
<xs:element name = "BackplaneType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Card">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "RequiresDaughterBoard" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Model" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SerialNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "LocationWithinContainer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PartNumber" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "CardType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "HardwareVersion" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OperationalStatus" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FWManufacturer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Manufacturer" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfSlots" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NoOfCommunicationConnectors" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "SoftwareIdentity" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_CommunicationConnector" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_FlashDevice" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_PhysicalMemory" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Card" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_CommunicationConnector">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ConnectorType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_FlashDevice">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FlashDeviceType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Size" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPartitions" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ChipCount" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Removable" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_FlashPartition" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
```

```
</xs:element>
<xs:element name = "Cisco_FlashPartition">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Upgrade" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NeedsErasure" type = "xs:boolean" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PartitionStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "unknown"/>
<xs:enumeration value = "readOnly"/>
<xs:enumeration value = "runFromFlash"/>
<xs:enumeration value = "readWrite"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "FileSystemSize" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "AvailableSpace" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileCount" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_FlashFile" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_FlashFile">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileSize" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "FileStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "unknown"/>
<xs:enumeration value = "deleted"/>
<xs:enumeration value = "invalidChecksum"/>
<xs:enumeration value = "valid"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Checksum" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_PhysicalMemory">
<xs:complexType>
<xs:sequence>
<xs:element name = "MemoryType" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "nvRam"/>
<xs:enumeration value = "NVRAM"/>
<xs:enumeration value = "processorRam"/>
<xs:enumeration value = "RAM"/>
<xs:enumeration value = "ROM"/>
<xs:enumeration value = "FEPROM"/>
<xs:enumeration value = "BRAM"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Capacity" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
```

```
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_NetworkElement">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PrimaryOwnerName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PhysicalPosition" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SysObjectId" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SysUpTime" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OfficialHostName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPorts" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_LogicalModule" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_Port" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_MemoryPool" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_IfEntry" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_IPProtocolEndpoint" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_PEHasIfEntry" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_LogicalModule">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ModuleNumber" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ModuleType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "EnabledStatus" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NumberOfPorts" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "Cisco_Port" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_LogicalModule" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "Cisco_OSElement" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_Port">
<xs:complexType>
<xs:sequence>
<xs:element name = "PortNumber" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PortType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "IfInstanceID" type = "xs:integer" minOccurs = "0" maxOccurs = "unbounded"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_MemoryPool">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PoolType" type = "xs:integer" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "DynamicPoolType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "AlternatePoolType" type = "xs:string" minOccurs = "0" maxOccurs = “1"/>
<xs:element name = "IsValid" type = "xs:boolean" minOcurs = "0" maxOccurs = "1"/>
<xs:element name = "Allocated" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Free" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "LargestFree" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
```

```
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
<!--PoolType ValueMap  {"0", "1", "2", "3", "4", "5", "65536"},
Values {"Unknown", "Processor", "I/O", "PCI", "Fast", "Multibus", "Dynamic"},
-->
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_OSElement">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "OSFamily" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Version" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_IfEntry">
<xs:complexType>
<xs:sequence>
<xs:element name = "InstanceID" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "InstanceName" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "ProtocolType" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Speed" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "RequestedStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "up"/>
<xs:enumeration value = "down"/>
<xs:enumeration value = "testing"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "OperationalStatus" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "Up"/>
<xs:enumeration value = "Down"/>
<xs:enumeration value = "Testing"/>
<xs:enumeration value = "Unknown"/>
<xs:enumeration value = "Dormant"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "Description" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "PhysicalAddress" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "NetworkAddress" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_IPProtocolEndpoint">
<xs:complexType>
<xs:sequence>
<xs:element name = "Address" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "SubnetMask" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "DefaultGateway" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element ref = "AdditionalInformation" minOccurs = "0" maxOccurs = "unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_PEHasIfEntry">
<xs:complexType>
```

```
<xs:sequence>
<xs:element name = "Cisco_IPProtocolEndpoint" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Cisco_IfEntry" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "Cisco_ComputerSystemPackage">
<xs:complexType>
<xs:sequence>
<xs:element name = "Antecedent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<xs:element name = "Dependent" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
<!--
Antecedent is the InstanceID from Cisco_Chassis Element
Dependent is the InstanceID from Cisco_NetworkElement
-->
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "SoftwareIdentity">
<xs:complexType>
<xs:sequence>
<xs:element name = "Classification" minOccurs = "0" maxOccurs = "1">
<xs:simpleType>
<xs:restriction base = "xs:string">
<xs:enumeration value = "Firmware"/>
<xs:enumeration value = "Software"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name = "VersionString" type = "xs:string" minOccurs = "0" maxOccurs = "1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name = "AdditionalInformation">
<xs:complexType>
<xs:sequence>
<xs:element name = "AD" minOccurs = "0" maxOccurs = "unbounded">
<xs:complexType>
<xs:attribute name = "name" type = "xs:string"/>
<xs:attribute name = "value" type = "xs:string"/>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Detailed Description of the Inventory Schema

The inventory schema provides the structure for the inventory information exported from Resource Manager Essentials (RME). The schema divides inventory information into two groups:

- Physical Inventory
- Logical Inventory

The Physical Inventory contains the chassis information and related details for the device. The main elements in the schema for the physical inventory part are:

- Chassis (Cisco_Chassis
- Backplane (Cisco_ Backplane
- Card (Cisco_Card)

- CommunicationConnector (Cisco_CommunicationConnector)
- FlashDevice (Cisco_FlashDevice)
- FlashPartition (Cisco_FlashPartition)
- FlashFile (Cisco_FlashFile)
- .SoftwareIdentity (Cisco_SoftwareIdentity)
- PhysicalMemory (Cisco_PhysicalMemory)

The Logical Inventory part of the schema contains the details of the managed network element. The main elements in the schema for the logical inventory part are:

- .ManagedNetworkElement (Cisco_NetworkElement)
- LogicalModule (Cisco_LogicalModule)
- Port (Cisco_Port)
- MemoryPool (Cisco_MemoryPool)
- OSElement (Cisco_OSElement)
- IPProtocolEndpoint (Cisco_IPProtocolEndpoint)
- IfEntry (Cisco_IfEntry)
- Additional Information

Chassis (Cisco_Chassis

The Chassis class represents the physical elements that enclose other elements in the device and provide specific functions, such as a desktop, networking node, UPS, disk or tape storage, or a combination of these functions.

The following table describes the elements in Chassis:

Element	Description
InstanceID	Unique identifier.
Model	Chassis model / Chassis ID.
Version	Hardware version of the chassis
SerialNumber	Serial number associated with the chassis.
Type	Chassis type.
NumberOfSlots	Number of slots in a chassis.
NoOfCommunicationConnectors	Number of physical connectors in a chassis.

Chassis also contains the elements Card and Backplane.

Backplane (Cisco_ Backplane

Backplane is an instance of a backplane in a chassis. The following table describes the elements in Backplane:

Element	Description
BackplaneType	Type of backplane
Model	Model of the backplane
SerialNumber	Serial number of the backplane.

Card (Cisco_Card)

Card represents:

- A type of physical container that can be plugged into another card, motherboard, or hosting board
- A motherboard or hosting board in a chassis

This element includes any package capable of carrying signals and providing a mounting point for physical components such as chips, or other physical packages such as other cards. The following table describes the elements in Card:

Element	Description
InstanceID	Card number. This is used to correlate with the logical part of the card.
Model	Model of the card.
SerialNumber	Serial number of the card.
LocationWithinContainer	Number that indicates the physical slot number. This can be used as an index into a system slot table, irrespective of whether that slot is physically occupied or not.
PartNumber	Part number of the Hardware Component.
CardType	Type of the card (Card Type)
Description	Descriptive string used to describe the card.
OperationalStatus	Status of the card describing whether it is up or down
FWManufacturer	Manufacturer of the firmware
Manufacturer	Manufacturer of the hardware
NumberOfSlots	Number of slots in the card.
NoOfCommunicationConnectors	Number of ports in the card.

Apart from the elements described in the table above, the card element also contains reference to itself, which can represents a sub card. It also contains other elements such as CommunicationConnector and FlashDevice.

CommunicationConnector (Cisco_CommunicationConnector)

CommunicationConnector represents a physical port. The table below describes the elements in CommunicationConnector:

Element	Description
InstanceID	Indicates the connector number for the chassis or system.

Element	Description
ConnectorType	Type of the physical port.
Description	Descriptive string used to describe the card.

FlashDevice (Cisco_FlashDevice)

FlashDevice represents physical flash memory. Flash memory may reside on a PCMCIA card, line card, or any other type of card. FlashDevice may consist of one or more actual flash memory chips.

It also consists of reference to one or more flash partitions described in FlashPartition. The table below describes the elements in FlashDevice.

Element	Description
InstanceID	FlashDevice sequence number to index the flash devices within the table of initialized FlashDevices.
InstanceName	Name of FlashDevice. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name.
Size	Total size of FlashDevice. For a removable device, the size will be zero if the device has been removed.
NumberOfPartitions	Number of Flash partitions present in f FlashDevice
ChipCount	Total number of chips within FlashDevice. This element provides information to a network management station on how much chip information to expect. It also helps the management station to check the chip index against an upper limit when randomly retrieving chip information for a partition.
Description	Description of a FlashDevice. The description is meant to explain what FlashDevice is and its purpose.
Removable	Specifies whether FlashDeviceis removable. Typically, only PCMCIA Flash cards are treated as removable. Socketed Flash chips and Flash SIMM modules are not treated as removable.

FlashPartition (Cisco_FlashPartition)

FlashPartition corresponds to the Cisco-flash-mib. The elements in FlashPartiion are derived from the table of properties of ciscoFlashPartitionTable for each initialized flash partition.

When there is no explicit partitioning for a device, it is assumed that there is a single partition spanning the entire device exists. Therefore, a device always has at least one partition.

FlashPartition contains one or more FlashFileSystems as described in FlashFile. The table below describes the elements in FlashPartition.

Element	Description
InstanceID	FlashPartition sequence number used to index FlashPartitions within the table for initialized FlashPartitions.
InstanceName	FlashPartition name used to refer to a partition by the system.
PartitionStatus	Status of the partition.
Upgrade	Upgrade information for the partition. This helps to download new files into the partition, and is needed when the PartitionStatus is run from flash.

Element	Description
NeedsErasure	Boolean parameter indicating whether the partition requires to be erased before any write operations can occur.
Size	FlashPartition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize.
FreeSpace	Free space within aFlashPartition.
FileCount	Number of files stored in the file system.

FlashFile (Cisco_FlashFile)

FlashFile manages the storage and organization of files on a Flash memory device. The table below describes the elements in FlashFile

Element	Description
InstanceID	FlashFile sequence number used to index within a FlashPartition directory table.
FileSize	Size of the file in bytes.This size does not include the size of the filesystem file header.
FileStatus	Status of a file. A file could be explicitly deleted if the file system supports such a user command. Alternatively, an existing good file would be automatically deleted if another good file with the same name were copied in. Deleted files continue to occupy prime space in flash memory. A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space, or because of a network download failure) are also written with a bad checksum and marked as invalid.
Checksum	File checksum stored in the file header. This checksum is computed and stored when the file is written into Flash memory, and serves to validate the data written into Flash. Where the system generates and stores the checksum internally in hexadecimal form, checksum provides the checksum in a string form. Checksum is available for all valid and invalid-checksum files.
FileName	FlashFile name as specified by the user while copying the file to Flash memory. The name should not include the colon (:) character as it is a special separator character used to separate the device name, partition name, and the file name.

.SoftwareIdentity (Cisco_SoftwareIdentity)

SoftwareIdentity provides the hardware and firmware version of the card. The table below describes elements in SoftwareIdentity.

Element	Description
Classification	Specifies whether the information is for hardware or firmware.
VersionString	Version information for software or firmware.

PhysicalMemory (Cisco_PhysicalMemory)

PhysicalMemory specifies the memory type and capacity of the device. The table below describes elements in PhysicalMemory.

Element	Description
MemoryType	Specifies the type of memory, that is whether RAM, ROM, or NVRAM.
Capacity	Capacity in bytes.

.ManagedNetworkElement (Cisco_NetworkElement)

ManagedNetworkElement is the entity that contains all logical parts of the device, which the users can configure (such as Logical Module, Port, Interfaces, Software Image details, and Memory Pool). The table below describes elements in ManagedNetworkElement.

Element	Description
InstanceID	Index number assigned to the network element.
Description	Description of the network element. This description includes the full name and version identification of the system's hardware type, operating system, and networking software. The description can have only printable ASCII characters.
PrimaryOwnerName	Identification of the contact person for this managed node, and information on how to contact this person.
InstanceName	Administratively defined name for the network element.
PhysicalPosition	Physical location of the network element.
SysObjectId	Vendor's authoritative identification of the management subsystem contained in the element.
SysUpTime	Time in hundredths of a second since the network management portion of the element was last initialized.
OfficialHostName	Name of the device.
NumberOfPorts	Number of ports in the network element.

LogicalModule (Cisco_LogicalModule)

LogicalModule is the logical device corresponding to a line card in the network device.

For example, a line card in a switch is an instance of LogicalModule, associated with the ManagedNetworkElement, in this case the switch. LogicalModule is not necessarily independently managed.

To represent a sub module, LogicalModule contains a reference to itself. It also contains Port and the OSElement. The table below describes the other elements in LogicalModule.

Element	Description
InstanceID	Index that correlates the physical card and the logical module. This helps to correlate the physical card to logical card details.
ModuleNumber	Number assigned to the module by its parent ManagedNetworkElement.

Element	Description
ModuleType	Type or model of the module.
InstanceName	Name of the logical module.
EnabledStatus	Status of the module, that is whether it is up or down.
NumberOfPorts	Number of ports in the logical module.

Port (Cisco_Port)

Port is the logical representation of network communications hardware - a physical connector and the setup or operation of the network chips, at the lowest layers of a network stack

For example, an Ethernet port on an Ethernet line card uses an instance of Port to represent its operational and logical properties. A port should be associated with either a LogicalModule or directly with a ManagedNetworkElement.

It also contains the element IPProtocolEndpoint. The table below describes the other elements in Port.

Element	Description
PortNumber	Number assigned to the port. Ports are often numbered relative to either a logical module or a network element.
PortType	Type of the port.
InstanceName	Name assigned to the port.
IfInstanceID	Index of the interface related to this port.

MemoryPool (Cisco_MemoryPool)

MemoryPool corresponds to entries to monitor entries. Each pool is a range of memory segregated by type or function. The table below describes the other elements in MemoryPool.

Element	Description
InstanceName	Name assigned to the MemoryPool.
PoolType	Dynamic type value assigned to a dynamic MemoryPool. This is valid only when the PoolType attribute has the value *Dynamic*. MemoryPools can be divided into two groups Predefined Pools and Dynamic Pools. For dynamic pools, the PoolType is set to the dynamic value (65536) and the DynamicPoolType is set to an integer value used to distinguish the various dynamic pool types.
DynamicPoolType	This attribute holds the dynamic type value assigned to a dynamic memory pool. It is only valid when the PoolType attribute has the value Dynamic (65536).
AlternatePoolType	Indicates whether this MemoryPool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If the value is set to zero, then this pool does not have an alternate. Otherwise the value is the same as the value of PoolType of the alternate pool.

Element	Description
IsValid	Indicates whether the other attributes in this MemoryPool contain accurate data. If an instance of this object has the value, False, (indicating an internal error condition), the values of the remaining objects in the instance may contain inaccurate information. That is, the reported values may be less than the actual values.
Used	Indicates the number of bytes from the MemoryPool that are currently in use by applications on the managed device.
Allocated	Indicates the number of bytes from the MemoryPool that are currently unused on the managed device.
Free	Indicates the largest number of contiguous bytes from the MemoryPool that are currently unused on the managed device.

OSElement (Cisco_OSElement)

OSElement represents the software element that is deployed to a network system and describes the software behind the operating system.The table below describes the other elements in OSElement.

Element	Description
InstanceName	Name of the OS image.
Family	Family of the OS component.
Version	Version of the OS.
Description	Description of the OS image.

IPProtocolEndpoint (Cisco_IPProtocolEndpoint)

IPProtocolEndpoint contains the subnet mask and default gateway information corresponding to the management IP Address.

Element	Description
Address	IP address of this endpoint, formatted according to the convention as defined in the AddressType property of this class.
SubnetMask	Mask for the IP address of this element, formatted according to the convention as defined in the AddressType property of this class (e.g., 255.255.252.0).
DefaultGateway	Default gateway address.

IfEntry (Cisco_IfEntry)

IfEntry represents the contents of an entry in the ifTable as defined in RFC 1213.

Element	Description
InstanceID	Index in the interface table defined in RFC 1213 for the entry containing the interface attributes of this object.
InstanceName	ifName attribute in the interface table defined in RFC 1213.

Element	Description
IfType	Interface type enumeration taken from the IANA definition of ifType.
IfSpeed	Estimate of the current bandwidth of the interface in bits per second. In cases, where the current bandwidth cannot be given, the nominal bandwidth should be specified.
IfAdminStatus	Desired state of the interface.
IfOperStatus	Current operational status of the interface.
Description	Description of the interface.
PhysicalAddress	Hardware address of the interface.
NetworkAddress	Network address of the interface.

Additional Information

AdditionalInformation is used to describe device specific information. It contains name and value attributes for elements specific to the device.

Class	Element	AdditionalInformation Tag
Cisco Call Manager	Cisco_NetworkElement	ActivePhones, InActivePhones, ActiveGateways, InActiveGateways, CallManagerIndex, CallManagerName, CallManagerDescription, CallManagerVersion, CallManagerStatus
	Cisco_Chassis	ApplicationPackageIndex, PackageManufacturer, Productname, Packageversion, Package SerialNumber
Cisco FastSwitch With_Module	Cisco_NetworkElement	FwdEngRev, BoardRev, SwitchPortNumber , SharedPortNumber, FirmwareSource
	Cisco_FlashDevice	FlashBankStatus
	Cisco_Card	InstanceID, ID
Cisco Firewall	None	None
Cisco IPX-IGX-BPX	Cisco_Chassis	InstanceName , Number
	Cisco_Card	SecondarySwRev, slotIndex, RAMId, ROMId, BRAMId, BOOTId, LocationWithinContainer, SecondaryStatus
	Cisco_Port	switchIfSlot,switchIfPort, SubPortNo, Status, Speed, PortType
Cisco LS1010 Switch	Cisco_Chassis	Slot0 (Type), Slot1(Type), AvailableSlots
	Cisco_NetworkElement	ConfigReg
	Cisco_PhysicalMemory	NVRAMUsed, RomVersion
Cisco MGX	Cisco_Chassis	Name, switchIfSlot, switchIfPort, SubPortNo, Status, Speed, PortType
Cisco Catalyst 3900 Switch	Cisco_Chassis	ModuleCount, Configuration, SwitchCount
	Cisco_Card	CiscoTsNumber, PermanentMAC, LocalMAC, CiscoTsModNumber , StackNo
Cisco Router 700 Series	Cisco_Chassis	MACAddress, PortCount, Type
Cisco Router	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
	Cisco_NetworkElement	Config

Class	Element	AdditionalInformation Tag
Cisco Catalyst IOS Switch	Cisco_Chassis	MACAddress, PortCount, Type
	Cisco_Card	FlashSize,FlashFree,FlashCard
	Cisco_Chassis	Config
	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
Cisco Catalyst L2L3 Switch	Cisco_Chassis	Slot0, Slot1 , MACAddress, PortCount, Type
	Cisco_NetworkElement	Config
	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
Cisco VPN 3000 Concentrators	Cisco_Chassis	PowerSupply1Type, PowerSuppy2Type, RAMSize
	Cisco_Card	LocationWithinContainer, CryptoHardwareType, SepState, DSPCodeVersion
Cisco Catalyst Switch	Cisco_Chassis	PowerSupply1, PowerSupply2 , MgmtType, BroadcastAddress, AvailableSlots
	Cisco_Card	ModuleIndex, RedundantModule, ModuleSubType
	Cisco_LogicalModule	moduleIndex,ModuleIPAddress
Cisco Optical Switches	Cisco_NetworkElement	RFUnitDetected, RFUnitID, RFUnitState, RFPeerUnitID, RFPeerUnitState, ActivateRF, ManualSwitchPermitted , StartupSyncStatus, RunningSyncStatus
	Cisco_PhysicalMemory	NVRAMUsed
Cisco FastSwitch	Cisco_NetworkElement	FwdEngRev, BoardRev, SwitchPortNumber , SharedPortNumber, FirmwareSource
	Cisco_FlashDevice	FlashBankStatus
	Cisco_Chassis	EPROMRev
	Cisco_CommunicationConnector	swPortIndex , PortTableSize, RevName, Type
Cisco Content Service Switch	None	None
Cisco Aironet	Cisco_PhysicalMemory	NVRAMUsed, ROMVersion
	Cisco_NetworkElement	Config
Cisco NAM	None	None
Cisco Management Engines	None	None

Overview: cwcli inventory Command

The `cwcli inventory` is a RME Device Management application command line tool. This tool supports the following features:

- You can check the specified device credentials for the RME devices.
- You can export device credentials of one or more RME devices in clear text.
- You can delete the specified RME devices.
- You can view the RME devices state.

The **`cwcli inventory`** command is located in the following directories, where *install_dir* is the directory in which CiscoWorks is installed:

- On UNIX systems, /opt/CSCOpx/bin
- On Windows systems, *install_dir*\CSCOpx\bin

  The default install directory is C:\Program Files.

If you install RME on an NTFS partition on Windows, only users in the administrator or casuser group can access **`cwcli inventory`**.

You can also perform the **`cwcli inventory`** tasks using the servlet. You will have to upload a payload XML file, which contains the **`cwcli inventory`** command arguments and CiscoWorks user credentials.

You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

`perl` *samplepost.pl* **`http://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`perl` *samplepost.pl* **`https://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>

<command>

cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...

</command>

</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

`http://`*rme-server:rme-port***`/rme/cwcli?command=cwcli inventory`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`https://`*rme-server:rme-port***`/rme/cwcli?command=cwcli inventory`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTPS mode is 443.

The BAse64 encoded for "admin" is YWRtaW4=.

The URL encode for,

- Double quotes (") is %22

- Percentage sign (%) is %25

Using the cwcli inventory Command

The command line syntax of the application is in the following format:

`cwcli inventory` *command GlobalArguments AppSpecificArguments*

The command line syntax of the application is in the following format:

`cwcli export` *command GlobalArguments AppSpecificArguments*

- **`cwcli inventory`** is the CiscoWorks command line interface for:
  - Checking the specified device credentials for the RME devices.
  - Exporting device credentials of one or more RME devices in clear text.
  - Deleting the specified RME devices.
  - Viewing the RME devices state.
- *Command* specifies which core operation is to be performed.
- *GlobalArguments* are the additional parameters required for each core command.
- *AppSpecificArguments* are the optional parameters, which modify the behavior of the specific **`cwcli inventory`** core command.

The order of the arguments and arguments are not important. However, you must enter the core command immediately after **`cwcli inventory`**.

The following sections describe:

- The **`cwcli inventory`** commands (See cwcli inventory Commands)
- The mandatory and optional arguments (See cwcli inventory Global Arguments)

On UNIX, you can view the **`cwcli inventory`** man pages by setting the MANPATH to /opt/CSCOpx/man. The man pages to launch the **`cwcli inventory`** are:

- man cwinventory-cda to launch the **`cwcli inventory cda`** command.
- man cwinventory-**`delete`** to launch the **`cwcli inventory delete`** command.
- man cwinventory-export to launch the **`cwcli inventory export`** command.
- man cwinventory-state to launch the **`cwcli inventory getdevicestate`** command

cwcli inventory Commands

The following table lists the command part of the **`cwcli inventory`** syntax:

Command	Description
`cwcli inventory cda`	You can check the specified device credentials for the RME devices. See Running the cwcli inventory cda Command
`cwcli inventory crmexport`	You can export device credentials of one or more RME devices in clear text. See Running the cwcli inventory crmexport Command

`cwcli inventory deletedevice`	You can delete the specified RME devices. See Running the cwcli inventory deletedevice Command
`cwcli inventory getdevicestate`	You can view the RME devices state. See Running the cwcli inventory getdevicestate Command

cwcli inventory Global Arguments

The following describes the mandatory and optional global arguments for **`cwcli inventory`**:

Argument	Description	Usage Notes
`-u` *user*	Enter a valid CiscoWorks username.	Mandatory.
`-p` *password*	Enter the password for the username.	Mandatory. You can provide this as part of argument or you can enter the password when you get the password prompt. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.
{**`-device`** *name* | **`-view`** *name* | **`-device`** *list* **`-view`** *name*| **`-ipaddress`** *list*}	**`device`** *name*—Enter the Display name of the device that you have added in the Device and Credentials database (Common Services > Device and Credentials > Device Management)	Mandatory • You can enter multiple device list separated using a comma. For example, if there are two devices with Display Names Rtr12 and Rtr13, using Rtr% will display both the devices. • To include all the devices in the RME, use the wild card character "%". For example, To use all the devices, use **`-device`** %.
	`view` *name*—Enter the Device Group name.	Mandatory You can enter multiple group name separated using a comma. For view name, you have to enter the fully qualified path as in the Group Administration GUI. For example, **`-view`** "/RME@*ciscoworks_servername*/ All Devices"
	`device` *list* **`view`** *name*—Enter the Display name and the Device Group name.	Mandatory.
	`ipaddress` *list*—Enter the device IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated.	Mandatory. You cannot use this option with **`-device`**, **`-view`**, or **`-input`**. Also, you cannot specify wildcard characters.

Argument	Description	Usage Notes
[`-d` *debug_level*]	Enter the debug level.	Optional. *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.
[`-m` *email*]	Specify an e-mail address to send the results.	Optional. *email* is one or more e-mail addresses for notification. They can be separated by a space or comma.
[`-l` *logfile*]	Specify a file to which this command has to write log messages. The default log filename is cli.log. The default log directory is: On Windows: *NMSROOT*\log Where *NMSROOT* is the CiscoWorks installed directory. On Solaris: /var/adm/CSCOpx/log	Optional. Use the relative pathname to specify the *log_filename*.
-help	Displays command usage information	None.

Running the cwcli inventory cda Command

You can use this command to check the following device credentials:

- SNMP Read Community String—SNMP version 2 read community string.
- SNMP Write Community String—SNMP version 2 write community string.
- SNMP Version 3—SNMP version 3 username and password.
- Telnet—Telnet username and password.
- Telnet Enable Mode User Name and Password—Telnet username and password in Enable mode.
- SSH—SSH username and password.
- SSH Enable Mode User Name and Password—SSH username and password in Enable mode.

You can update these credentials using **Common Services > Device and Credentials > Device Management**.

The command syntax for `cwcli inventory cda` is:

cwcli inventory cda -u *userid* **-p** *password* {**-invoke** | **-status**} [**-credType** *credTypeL*ist] {**-device** *list* | **-view** *name* | **-device** *list* **-view** *name* | **ipaddress** *list*} [**-d** *debuglevel*] [**-m** *email*] [**-help**] [**-l** *logfile*]

Arguments in square brackets ([]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **`cwcli inventory cda`** command.

The other common arguments used by **`cwcli export`** are explained in Using the cwcli export Command

:

Argument	Description	Usage Notes
{**`-invoke`** | **`-status`**}	Invoke—Invokes the Check Device Attribute operation. Status—Displays the check device attributes result.	Mandatory. These arguments are mutually exclusive. You cannot run **`-invoke`** and **`-status`** together. After using the **`-invoke`** argument to the check device attribute you must run the command again with -status argument to view the result. If you are checking the device credentials for same devices and for same set of credentials, then you can use **`-invoke`** argument only once. If you are checking the device credentials for different devices and different credentials then you must use **`-invoke`** argument first and then you must use **`-status`**.
{**`-credType`** *credTypeList*}	Enter the device credentials for which you want to view the status. You can use the following arguments to view the different credentials status: • 0 —Enter **0** to view all credentials status. • 1 — Enter **1** to view status for Read Community. • 2 — Enter **2** to view status for Write Community. • 3 — Enter **3** to view status for SNMP version 3 username and password. • 4 — Enter **4** to view status for Telnet username and password. • 5 — Enter **5** to view status for Telnet username and password in Enable mode. • 6 — Enter **6** to view status for SSH username and password. • 7 — Enter **7** to view status for SSH username and password in Enable mode. You can specify multiple arguments separated by comma to check multiple credentials	Mandatory. If you do not specify the credentials type, all credentials status are displayed.

Argument	Description	Usage Notes
Command Argument for Inventory CDA `createjob`		
{`-device` *comma_separated_devicelist* }|{`-view` *device_view_name*}	`-device` *comma_separated_devicelist* - Specify devices to be used for the job. The *comma_separated_devicelist* is list of devices. `-view` *device_view_name* Specify the device view to be used for the job. The *device_view_name* is the name of a device view.	Mandatory. These arguments are mutually exclusive. You cannot run `-device` and `-view` together. `cwcli inventory cda createjob -u` *Username* `-p` *Password* `-device` *Device 1*, *Device 2* |`-view` *device_view_name*, `-schedule` *Schedule* `-scheduletype` *Schedule Type*
[{`-schedule` *MM/dd/yyyy:HH:mm:ss* `-scheduletype` *Once* | *Daily* | *Weekly* | *Monthly* | *LastDayOfMonth* | *6hourly* | *12hourly*}]	You can specify the date and time as well as the frequency of the CDA job. • To specify the date and time when you want to run the CDA job, use the `schedule` option. • To specify the frequency of the job use the `scheduletype` option. You have to set both the `schedule` and `scheduletype` options for a scheduled job. You do not have to set the `schedule` and `scheduletype` for an Immediate job.	Optional. *scheduletype* can have any of the following values: • Once • 6hourly • 12hourly • Daily • Weekly • Monthly If the `schedule` option is not specified, the job will be created as an immediate job.
[`-input` *argFile*]	Input file containing the details of the subcommands to be used for a job creation.	Optional If you are specifying the argument file, you need not specify the arguments in the command line. `cwcli inventory cda -u` *admin* `-p` *admin* [`-input` *argFile*]
[`-description` *JobDescription*]	Gives details of the job.	*JobDescription* is a user-defined entry describing the job details.
[`-notificationmail` *comma_separated_email_list*]	Specify the email addresses to which the configuration job will sends status notices.	Optional Separate multiple addresses with commas.

Argument	Description	Usage Notes
{**`-credType`** *credentialList*}	Enter the device credentials for which you want to create a job. You can use the following arguments to view the different credentials status: • 0 —Enter **0** to view all credentials status. (ALL). • 1 — Enter **1** to view status for Read Community. • 2 — Enter **2** to view status for Write Community. • 3 — Enter **3** to view status for SNMP version 3 username and password. • 4 — Enter **4** to view status for Telnet username and password. • 5 — Enter **5** to view status for Telnet username and password in Enable mode. • 6 — Enter **6** to view status for SSH username and password. • 7 — Enter **7** to view status for SSH username and password in Enable mode. You can specify multiple arguments separated by comma to check multiple credentials.	Mandatory If you do not specify the credentials type, all credentials status are displayed.
Command Argument for Inventory CDA `stopjob`		
{**`-id`** *Job ID*}	You can stop only one job at a time. You can stop a CDA job that is in scheduled as well as running state.	Mandatory Use this command to stop an Inventory CDA job that is scheduled. **`cwcli inventory cda stopjob -u`** *userid* **`-p`** *password* {**`-id`** *jobID*}
Command Argument for Inventory CDA `deletejob` and `jobdetails`		
{**`-id`** *Job IDs*}	You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas.	Mandatory Inventory CDA deletejob command: **`cwcli inventory cda deletejob -u`** *userid* **`-p`** *password* {**`-id`** *jobID1, jobID2..*} Inventory CDA jobdetails command: **`cwcli inventory cda jobdetails -u`** *userid* **`-p`** *password* {**`-id`** *jobID1, jobID2..*}

Argument	Description	Usage Notes
Command Argument for `Inventory CDA listjobs`		
[**`-jobstatus`** *status*]	You can specify the status of the job. This can be: - All jobs - Running jobs - Completed jobs - Pending jobs.	Optional. **`cwcli inventory cda listjobs -u`** *Username* **`-p`** *Password* [**`-jobstatus`** *A, R, C, P*]
Command Arguments for Inventory CDA `jobresults`		
{**`-id`** *Job ID, Job ID*}	You can list the results of more than one job at a time. Enter the job IDs separated by commas.	**`cwcli inventory cda jobresults -u`** *Username* **`-p`** *Password* **`-id`** *"Job ID 1" , "Job ID 2" , "Job ID 3"*
[**`-csvoutput`** *filepath*]	You can specify the fully qualified pathname for saving the job results.	If you do not specify this argument, the job results appear in the console itself. If the specified path does not exist, the job results are stored in the default location. **`cwcli inventory cda jobresult -u`** *admin* **`-p`** *admin* {**`-jobid`** *jobID*} [**`-csvoutput`** *filepath*]

The Table 19-1 maps the device credentials that you have entered in the Device and Credentials (**Common Services > Device and Credentials > Device Management**) database and the credentials that appear in the `cwcli inventory cda` command:

Table 19-1 Credentials Mapping

Credentials in Device and Credentials Database	Credentials displayed in `cwcli inventory cda`
Device Name	deviceName
SNMP V2C RO Community String	ro
SNMP V2C RW Community String	rw
SNMP V3 Username and Password	snmpv3
Primary Credentials Username	telnet
Primary Credentials Username and Primary Enable Password	telnetEnable
Primary Credentials Username	ssh
Primary Credentials Username and Primary Enable Password	sshEnable

The Table 19-2 describes the Credential Verification Report Status messages:

Table 19-2 Understanding Credential Verification Report

Status Message	Description
OK	Check for device credentials completed. The device credentials data in the Device and Credential Repository matches the physical device credentials.
No authentication configured	Device was not configured with authentication mechanism (Telnet/LocalUsername/TACACS). RME was able to telnet and log into the device successfully with out using the values entered in the Device and Credential Repository.
Incorrect	Check for device credentials completed. The device credentials data in the Device and Credential Repository does not match with the physical device credentials for one of the following reasons: • The device credentials data in Device and Credential Repository is not correct. • The device is unreachable or offline. • One of the interfaces on the device is down.
No Data Yet	Check for device credentials is in progress.
Did Not Try	Check for device credentials is not performed for one of the following reasons: • A Telnet password does not exist, so could not login to the device. • Device Telnet login mode failed, so enable mode login is not attempted.
No Value To Test	Check for device credentials is not performed because you have not entered the device credentials data.
Not Supported	Check for Telnet passwords is not performed because Telnet credential checking is not supported on this device.
Failed	Check failed because a Telnet session could not be established due to a not responding device.
Not Selected For Verification	Protocol was not selected for verification.

Usage Examples for cwcli inventory cda Command

This section provides some examples of usage for the **`cwcli inventory cda`** command.

Example 1: Invoking the Check Device Attributes

`cwcli inventory cda -u` *admin* **`-p`** *admin* **`-invoke -device`** 3750-stack

The command output is:

```
CDA invoked for given device and credType list

SUMMARY

========

        Successful: CDA: Success
```

Example 2: Checking the read and write device credentials for multiple devices

```
cwcli inventory cda -u admin -p admin -device 3750-stack, rtr% -credtype 1,2 -status

CDA Status :

============

deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable

25 | rtr10005 | OK | OK |  |  |  |  |

27 | 3750-stack | OK | OK |  |  |  |  |

32 | rtr10K | No Data Yet | No Data Yet |  |  |  |  |

SUMMARY

========

        Successful: CDA: Success
```

Example 3: Checking all device credentials for a group

```
cwcli inventory cda -u admin -p admin -view "/RME@ciscoworksservername/Pre-deployed"
-status

CDA Status:

==========

deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable

29 | v2 | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No Data
Yet | No Data Yet

SUMMARY

========

        Successful: CDA: Success
```

Example 4: Checking device credentials for a device using the cwcli get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter this in your browser:

```
http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory cda -u admin -p
YWRtaW4= -device 10.10.10.12 -status
```

The output for this appears on your console:

```
<!-- Processing Starts  -->

CDA Status :

============

deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnable

12 | 10.10.10.12 | OK | OK | No Value To Test | Incorrect | Did Not Try | Failed | Did
Not Try


SUMMARY
```

```
========

Successful: CDA: Success

<!-- Processing complete -->
```

Example 5: Checking device credentials for a device using the cwcli post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *cda.xml* contains:

```
<payload>

   <command>

     cwcli inventory cda -u admin -p YWRtaW4=  -device 10.10.16.20 -status

   </command>

</payload>
```

At the command prompt enter:

perl *samplepost.pl* **http://ciscowork_servername:1741/rme/cwcli** *cda.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->

CDA Status :

============

deviceId | deviceName | ro | rw | snmpv3 | telnet | telnetEnable | ssh | sshEnab

le

71 | 10.10.16.20 | No Data Yet | No Data Yet | No Data Yet | No Data Yet | No

Data Yet | No Data Yet | No Data Yet


SUMMARY

========

        Successful: CDA: Success

<!-- Processing complete -->
```

Example 6: Creating a job using cwcli inventory cda createjob command

```
cwcli inventory cda createjob -u admin -p admin - Cat6230, Cat4500 | -view myview
-schedule 03/23/2007:12:15:01 -scheduletype Once
```

This command creates a cda job for the devices Cat6230 and Cat4500 in the view myview and scheduled for 23rd march 2007 at 12:15 pm with schedule type specified as Once.

Example 7: Stopping a cwcli inventory cda job using stopjob command

There is a job 1098, which is currently running. You can use this command to stop the job 1098.

```
cwcli inventory cda stopjob -u admin -p admin -id 1098
```

Example 8: Deleting cwcli inventory cda jobs using deletejob command

There are two jobs 1057 and 1058 scheduled. You can use this command to stop the two jobs.

```
cwcli inventory cda deletejob -u admin -p admin -id 1057,1058
```

Example 9: Getting details of jobs using cwcli inventory cda jobdetails command

There are two jobs 1001 and 1002 that are scheduled. You can use this command to list the details of both the jobs:

```
cwcli inventory cda jobdetails -u admin -p admin -id 1001, 1002
```

Example 10: Listing the cda jobs based on the status using the listjobs command

```
cwcli inventory cda listjobs -u admin -p admin -jobstatus R, C
```

Use this command to list those jobs whose status is Running or Completed.

Example 11: Obtaining results of jobs using jobresults comand

There are two jobs 1023 and 1024 that are completed. You can use this command to save the results of these jobs to the specified location.

```
cwcli inventory cda jobresult -u admin -p admin -jobid 1023, 1024 -csvoutput
C:/jobs/results
```

Running the cwcli inventory crmexport Command

You can use this command to export RME device credentials in CSV or XML format.

The command syntax for **`cwcli inventory crmexport`** is:

`cwcli inventory crmexport -u` *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] {**`-device`** *list* | **`-view`** *name* | **`-device`** *list* **`-view`** *name*} [**`ipaddress`** *list*] {**`-filetype`** *format* | **`-filename`** *outputfile*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **`cwcli inventory crmexport`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli inventory Command.

Argument	Description	Usage Notes
{**`-filetype`** *format* }	**`-filetype`** *format* —Enter the file format to export, either XML or CSV.	Mandatory. The default CSV file format version is 3.0.
{ **`-filename`** *outputfile* }	**`-filename`** *outputfile*—Enter the filename.	Mandatory. Specifies the name of the file to which the device credentials information is to be exported on CiscoWorks server. If you are using **`cwcli`** remotely (get or post request), by default the output file is available at this location on CiscoWorks server: On Windows: *NMSROOT*\MDC\tomcat Where, *NMSROOT* is the CiscoWorks installed directory. On Solaris: /opt/CSCOpx/objects/dmgt

Usage Examples for cwcli inventory crmexport Command

This section provides some examples of usage for the **`cwcli inventory crmexport`** command.

Example 1: Exporting device credentials of all RME devices in XML format

`cwcli inventory crmexport -device` % **`-filetype`** *xml* **`-filename`** *crmexport-xml* **`-u`** *admin* **`-p`** *admin*

```
SUMMARY

======== Successful: Export: Success
```

The RME device credentials are exported into a file, *crmexport-xml* in XML format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 2: Exporting device credentials of all RME devices in Normal State in CSV format

`cwcli inventory crmexport -view` "*/RME@ciscoworksservername/Normal Devices*" **`-filetype`** *csv* **`-filename`** *crmexport-csv* **`-u`** *admin* **`-p`** *admin*

```
SUMMARY

========

         Successful: Export: Success
```

The RME device credentials for devices that are in Normal state are exported into a file, *crmexport-csv* in CSV version 3.0 format. The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Example 3: Exporting device credentials of all RME devices using cwcli get request method

The password that you enter here must be in base64 encoded.

In this example,

- *YWRtaW4=* is the base64 encoded password for admin.
- %25 is the URL encode for "%"

Enter this in your browser:

http://*ciscowork_servername:***1741/rme/cwcli?command=cwcli inventory crmexport -u** *admin* **-p** *YWRtaW4=* **-device** *%25* **-filetype** *xml* **-filename** *getxml*

The output is written in the *getxml* file. The *getxml* file is located:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the CiscoWorks installed directory.

On Solaris:

/opt/CSCOpx/objects/dmgt

Example 4: Exporting device credentials of all RME devices using cwcli post request method

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *crmexport.xml* contains:

```
<payload>

   <command>

    cwcli inventory crmexport -u admin -p YWRtaW4=  -device 10.66.162.208 -filetype xml
-filename /opt/CSCOpx/crmexport-xml

   </command>

</payload>
```

At the command prompt enter:

perl *samplepost.pl* **http://ciscowork_servername:1741/rme/cwcli** *crmexport.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
SUMMARY

========

        Successful: Export: Success
```

The RME device credentials are exported into a file, *crmexport-xml* in XML format. This file is created in the /opt/CSCOpx directory. By default, the specified file is created in this location:

On Windows:

NMSROOT\MDC\tomcat

Where, *NMSROOT* is the CiscoWorks installed directory.

On Solaris:

/opt/CSCOpx/objects/dmgt

The credentials that are exported depends on the data that you have provided when you added the devices to Device Credentials Repository.

Running the cwcli inventory deletedevice Command

You can use this command to delete devices from RME.

The device information will be retained in the Device Credentials Repository. This information will not be removed till you delete the device from Device Credentials Repository.

The command syntax for **`cwcli inventory deletedevice`** is:

`cwcli inventory deletedevice -u` *userid* **`-p`** *password* [**`-d`** *debuglevel*] [**`-m`** *email*] [**`-l`** *logfile*] [**`-view`** *name*] {**`-device`** *list* | **`-input`** *inputfile* | **`ipaddress`** *list*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **`cwcli inventory deletedevice`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli export Command.

Argument	Description	Usage Notes
`-input` *inputfile*	**`-input`** *inputfile*—Enter the full path of the file containing comma-separated list of device display name as entered in Device Credentials Repository. The input file should be of this format: **`-device`** 1.1.1.1,2.2.2.2,3.3.3.3 or **`-device`** 1.1.1.1 **`-device`** 2.2.2.2 **`-device`** 3.3.3.3	Mandatory You must also enter the file format either CSV or txt.

Usage Examples for cwcli inventory deletedevice Command

This section provides some examples of usage for the **`cwcli inventory deletedevice`** command.

Example 1: To delete a device

`cwcli inventory deletedevice -u` *admin* **`-p`** *admin* **`-device`** *10.76.10.10*

```
<cwcli> INFO - Total number of devices deleted successfully: 1

SUMMARY

========

        Successful: Delete Device: Success
```

Example 2: To delete devices listed in a file

The input file, deletedevice contains list of device Display Name separated by a comma:

`-device` 3750-stack,rtr1000,rtr10005

`cwcli inventory deletedevice -u` *admin* **`-p`** *admin* **`-input`** *deletedevice.csv*

Example 3: To delete devices using cwcli get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter the following in your browser:

`http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory deletedevice -u` *admin* **`-p`** *YWRtaW4=* **`-device`** *10.10.10.41,10.10.10.51*

The output for this appears on your console:

```
<!-- Processing Starts  -->

<cwcli> INFO - Total number of devices deleted successfully: 2

SUMMARY

========

        Successful: Delete Device: Success

<!-- Processing complete -->
```

Example 4: To delete devices using cwcli post request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

The payload file, *deletedevicestate.xml* contains:

```
<payload>

   <command>

     cwcli inventory deletedevice -u admin -p YWRtaW4=  -device
10.77.9.10,10.77.9.18,10.76.8.6

   </command>

</payload>
```

At the command prompt enter:

`perl` *samplepost.pl* **`http://doclab2:1741/rme/cwcli`** *deletedevice.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->

<cwcli> INFO - Total number of devices deleted successfully: 3


SUMMARY

========

        Successful: Delete Device: Success

<!-- Processing complete -->
```

Running the cwcli inventory getdevicestate Command

You can use this command to view the RME device state.

The command syntax for **`cwcli inventory getdevicestate`** is:

`cwcli inventory getdevicestate -u` *userid* **`-p`** *password* [**`-d`** *debuglevel*]
[**`-m`** *email*] [**`-l`** *logfile*] [**`-view`** *name*] {**`-device`** *list* | **`-input`** *inputfile* | **`ipaddress`** *list*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({ }) are required. You must provide one argument from each group of arguments in curly braces ({ }) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used.

The following table describes the arguments that are specific to **`cwcli inventory getdevicestate`** command. The other common arguments used by **`cwcli export`** are explained in Using the cwcli inventory Command.

Argument	Description	Usage Notes
`-input` *inputfile*	**`-input`** *inputfile*—Enter the full path of the file containing comma-separated list of devices display name as entered in Device Credentials Repository. The input file should be of this format: **`-device`** 1.1.1.1,2.2.2.2,3.3.3.3 or **`-device`** 1.1.1.1 **`-device`** 2.2.2.2 **`-device`** 3.3.3.3	Mandatory You must also enter the file format either CSV or txt.

Usage Examples for cwcli inventory getdevicestate Command

This section provides some examples of usage for the **`cwcli inventory getdevicestate`** command.

Example 1: To view the device state of the RME devices

`cwcli inventory getdevicestate -u` *admin* **`-p`** *admin* **`-device`** *10.10.19.10,10.10.19.12*

```
<cwcli> INFO - Device State Information

DisplayName:Device State

10.10.19.10:PREDEPLOYED

10.10.19.12:NORMAL

SUMMARY

========

        Successful: getdevicestate: Success
```

Example 2: To view the devices state specified in a file

The input file, deletedevice contains list of device Display Name separated by a comma:

`-device` VG200,rtr1750,cat4000

`cwcli inventory deletedevice -u` *admin* **`-p`** *admin* **`-input`** *devicestate.csv*

Example 3: To view the devices state using get request

The password that you enter here must be in base64 encoded. In this example, *YWRtaW4=* is the base64 encoded password for admin.

Enter the following in your browser:

`http://ciscowork_servername:1741/rme/cwcli?command=cwcli inventory getdevicestate -u` *admin* **`-p`** *YWRtaW4=* **`-device`** *10.16.10.15,10.16.10.35*

The output for this appears on your console:

```
<!-- Processing Starts  -->

<cwcli> INFO - Device State Information

DisplayName:Device State

10.16.10.15:NORMAL

10.16.10.35:PREDEPLOYED


SUMMARY

========

        Successful: getdevicestate: Success

<!-- Processing complete -->.
```

Example 4: To view the RME device state using post request

The password that you enter here must be in base64 encoded. In this example, YWRtaW4= is the base64 encoded password for admin.

The payload file, *getdevicestate.xml* contains:

```
<payload>

   <command>

     cwcli inventory getdevicestate -u admin -p YWRtaW4=  -device 
12.20.12.26,10.6.12.21,12.18.10.129,10.7.9.13

   </command>

</payload>
```

At the command prompt enter:

`perl` *samplepost.pl* **`http://ciscowork_servername:1741/rme/cwcli`** *getdevicestate.xml*

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

```
<!-- Processing Starts  -->

<cwcli> INFO - Device State Information

DisplayName:Device State
```

```
12.18.13.129:ALIAS

10.7.9.13:PREDEPLOYED

10.6.12.21:NORMAL

12.20.12.26:NORMAL


SUMMARY

========

        Successful: getdevicestate: Success

<!-- Processing complete -->
```

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{        $str .= $_ ;
}
print $str ;
url_call($temp);
#-- Activate a CGI:
sub url_call
{
    my ($url) = @_;
    my $ua = new LWP::UserAgent;
    $ua->timeout(1000);
    # you can set timeout value depending on number of devices
    my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
    my $req = new HTTP::Request ('POST', $url, $hdr);
    $req->content($str);
    my $res = $ua->request ($req);
    my $result;

    if ($res->is_error)
    {
        print "ERROR : ", $res->code, " : ", $res->message, "\n";        $result = '';
    }
else {
        $result = $res->content;
           if($result =~ /Authorization error/)
        {           print "Authorization error\n";
                  }
    else {
    print $result ;
             }
     }
```

Overview: cwcli invreport Command

The **`cwcli invreport`** is a CiscoWorks command line tool which allows you to run previously created Inventory Custom Reports and also system reports. The supported output file format is Comma Separated Value (CSV).

The above command retrieves the inventory report in CSV format. The **`-file`** parameter stores the output in the file specified by *filename*. If you have not specified the filename, the output is stored at the following location:

NMSROOT\files\rme\jobs\inventory\reports\archives\*reportname_timestamp*.csv

You can:

- Use the **`-reportname`** argument to generate the report.

  This can be the name of:

  - An already defined custom template

    or

  - A system report name such as Detailed Device Report.

- Use the **`-input`** argument to specify a file containing the parameters for the report generation.

Note The **`-view`** argument is not allowed in the input file.

- Enable debug mode and set the debug level using the **`-d`** argument.
- E-mail the output to an e-mail recipient using the **`-m`** argument.
- Log the error messages to a file using the **`-l`** argument. The log and the output files are created in the current directory.
- List the existing reports with the **`-listreports`** argument.

Running the cwcli invreport Command

To use the **`cwcli invreport`** command, you must be able to run the cwcli command

You should be authorized to generate inventory reports.

The command syntax is:

cwcli invreport -u *userid* **-p** *password* [**-d** *debuglevel*] [**-m** *email*] [**-l** *logfile*] {**-listreports** | **-reportname** *name* {**-view** *viewname* | **-device** *list* | **-ipaddress** *list*} [**-file** *filename*] | **-input** *inputfile*}

Arguments in square brackets ([]) are optional; arguments in curly braces ({}) are required. You must provide one argument from each group of arguments in curly braces ({}) that is separated by vertical bars (|).

If you do not specify an optional argument, the default value configured for the system is used. Valid values for arguments are described in the following table:

Argument	Description	Usage Notes
-u *user*	Provide valid CiscoWorks username.	None.
-p *password*	Provide password for username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None.

Argument	Description	Usage Notes
[**-d** *debug_level*]	Set debug level.	Optional. *debug_level* is a number between 1 (the least information is sent to the debug output) and 5 (the most information is sent to the debug output). If you do not specify this argument, 4(INFO) is the default debug level.
[**-m** *email*]	Specify an e-mail address to send the results.	Optional. *email* is one or more e-mail addresses for notification. They can be separated by a space or comma.
[**-l** *log_filename*]	Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).	Optional. *log_filename* can be full pathname or filename in local directory.
[**-l** *log_filename*]	Logs the error messages and debug of messages of the invreport command, to the specified logfile name. If not specified, it will be written to default logs (invreports.log and cli.log).	Optional. *log_filename* can be full pathname or filename in local directory.

Argument	Description	Usage Notes
{**`-listreports`** | **`-reportname`** *name* {**`-view`** *viewname* | **`-device`** *list* | **`-ipaddress`** *list*} [**`-file`** *filename*] | **`-input`** *inputfile*}	Specify any one of the required arguments: • **`-listreports`** • **`-reportname`** • **`-input`**	**`-listreports`** argument lists out all Inventory system reports and custom reports templates. You can run this command if you have the required permissions to generate reports. **`-reportname`** *name* specifies the name of an already defined custom template or the name of a system report (such as Detailed Device Report) for which the CSV formatted report is to be generated. **`-input`** *inputfile* specifies the input file containing report parameters. The parameters in this file will be used to generate the CSV formatted report(s). This file should be located in the current directory or you can specify the complete path of the input file. **Note** The **`-view`** argument is not allowed in the input file.
	If you selected **`-reportname`** *name,* then specify any one of these arguments: – **`-view`** *viewname*. This confines the device search to the specified view. – **`-device`** *list.* This specifies one or more device names as a comma-separated list. Optionally, you can also specify **`-file`** *filename.* Name of the file where CSV formatted report will be stored. If you do not specify the location, the default location is *$NMSROOT*\files\rme\jobs\inventory\reports\archives\*reportname_timestamp*.csv – **`ipaddress`** *list*—This specifies IP4 address as entered in the Device and Credential Repository. You can enter multiple IP address with comma separated. You cannot use this option with **`-device`**, **`-view`** , or **`-input`**. Also, you cannot specify wildcard characters.	

Usage Examples

This section provides some examples of usage for the cwcli invreport command:

- Example 1
- Example 2

- Example 3
- Example 4
- Example 5
- Example 6

Example 1

`cwcli invreport -u` *admin* **`-p`** *admin* **`-reportname`** *"Detailed Device Report"* **`-device`** %

This generates Detailed Device Report for all devices and CSV file will be located at *$NMSROOT*\files\rme\jobs\inventory\reports\archives\Detailed Device Report_*timestamp*.csv

Example 2

`cwcli invreport -u` *admin* **`-p`** *admin* **`-reportname`** *"Detailed Device Report"* **`-device`** % **`-file`** *D:\cisco\CSCOpx\a.csv*

This generates Detailed Device Report, a system report, for all devices, and the result will be written to D:\cisco\CSCOpx\a.csv

Example 3

`cwcli invreport -u` *admin* **`-p`** *admin* **`-reportname`** *"Detailed Device Report"* **`-device`** % **`-file`** a.csv

This generates the Detailed Device Report, a system report, for all devices, and the result will be written to the file a.csv in the current directory (from where you are running this command).

Example 4

`cwcli invreport -u` *admin* **`-p`** *admin* **`-input`** *cliinputs.txt*

Generate the reports using the parameters provided in the file cliinputs.txt. Using **`-input`** argument you can run multiple reports at a time by providing parameters in the file.

Example 5

`cwcli invreport -u` *admin* **`-p`** *admin* **`-listreports`**

Displays a list of all Inventory system report and custom templates.

You can run this command if you have the required permissions to generate reports.

Example 6

`cwcli invcreport -u` *admin* **`-p`** *admin* **`-d`** 3 **`-m`** *xxx@yyy.com* **`-reportname`** *acmeinventory* **`-view`** acme **`-file`** *acmeinventory.txt*

Generates the report named acmeinventory, using the acme device view and the CSV formatted output will be written to acmeinventory.txt

You can place this file in the current directory (from where you are running the command).

cwcli invreport Remote Access

You can also perform the **`cwcli invreport`** tasks using the servlet. You will have to upload a payload XML file, which contains the **`cwcli invreport`** command arguments and CiscoWorks user credentials. You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the output either on the console or in the specified output file, if the credentials are correct and arguments are valid.

The name of the servlet is /rme/cwcli.

The following is the servlet to be invoked to execute any command:

For post request,

`perl` *samplepost.pl* **`http://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`perl` *samplepost.pl* **`https://`***rme-server:rme-port***`/rme/cwcli`** *payload_XML_file*

The default port for CiscoWorks server in HTTPS mode is 443.

The schema for creating the payload file in XML format is:

```
<payload>

<command>

cwcli inventory commandname -u user -p BAse64 encoded pwd -args1 arg1value...

</command>

</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

For get request,

`http://`*rme-server:rme-port***`/rme/cwcli?command=cwcli invreport`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTP mode is 1741.

If you have enabled SSL on CiscoWorks server, you can also use https protocol for secured connection.

`https://`*rme-server:rme-port***`/rme/cwcli?command=cwcli invreport`** *commandname* **`-u`** *user* **`-p`** *BAse64 encoded pwd -args1 arg1value...*

The default port for CiscoWorks server in HTTPS mode is 443.

The BAse64 encoded for “admin” is YWRtaW4=.

The URL encode for,

- Double quotes (“) is %22
- Percentage sign (%) is %25

Overview: cwcli netshow Command

You can invoke NetShow features from Command Line Interface (CLI).

The **`cwcli netshow`** commands let you use NetShow features from the command line. You can use the **`cwcli netshow`** commands to view, browse, create, delete, and cancel NetShow jobs.

You can also view the Command Sets assigned to each user by entering the command **`listcmdsets`** from CLI.

You can set the following job attributes using the command line option:

- E-mail Notification
- Job Based Password

- Execution Policy
- Approver List

However, the Administrator must define and assign the command sets to you, in the browser interface.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

If you have permission to run custom commands, you can run any of the following adhoc commands:

- **`show`**
- **`version`**
- **`where`**
- **`ping`**
- **`traceroute`**
- **`?`**

Administrator level users have all command sets assigned to them. However, only system-defined command sets are assigned to all users, by default. Other commands have to be assigned to the user by the Administrator. If any users create a command, it is automatically assigned to them.

Running cwcli netshow Command

The command syntax for running **`cwcli netshow`** commands is:

`cwcli netshow` *`common_arguments subcommands command_arguments`*

In the CLI version, you can provide the arguments in the (operating system shell) command line or in an input file. The input file provides you with flexibility and control over commands and command sets. You can specify the devices on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

For example, you can create a new netshow job with command sets, set1 and set2, and the custom commands, custom command 1 and custom command 2, by entering:

cwcli netshow createjob -u *Username* **-p** *Password* **-commandset** "*Command Set 1*"," *Command Set 2"* **-device** *Device 1*, *Device 2* **-customcmd** "*Custom command 1*"," *Custom command 2"* **-schedule** *Schedule* **-scheduletype** *Schedule Type*

Items in square brackets ([]) are optional; items in curly brackets ({}) are required.

The arguments are described in the following sections.

Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

Sub command	Description	Usage Notes	Example
createjob	Creates a new job that can be scheduled to run immediately or to be run sometime in the future. You can also specify the job attributes you want to enable.	Either use an input file containing the details of the subcommands or enter the full command syntax.	**cwcli netshow createjob -u** *Username* **-p** *Password* **-commandset** “*Command Set 1*”,” *Command Set 2*” **-device** “*Device Name 1*”, “*Device Name 2*” **-customcmd** “*Custom Command 1*”, “*Custom Command 2*” **-schedule** *Schedule* **-scheduletype** *Schedule Type* Or **cwcli netshow createjob -u** *Username* **-p** *Password* **-input** *Input File*
canceljob	Cancels an existing job.	Enter the job ID.	**cwcli netshow canceljob -u** ***Username*** **-p** *Password* **-id** ***“Job ID”***
deletejob	Deletes existing jobs.	Enter the job IDs separated by commas.	**cwcli netshow deletejob -u** *Username* **-p** *Password* **-id** “*Job ID 1*”,” *Job ID 2*”
jobdetails	Displays details of specified job.	Enter the job IDs separated by commas.	**cwcli netshow jobdetails -u** *Username* **-p** *Password* **-id** “*Job ID 1*”,”*Job ID 2*”, “*Job ID 3*”
listjobs	Displays a list of jobs created by the user and the job status.	Specify the type of jobs to be listed. The command type is case sensitive. The commands that you can use are: **A** —All jobs **R** —Running jobs **C** —Completed jobs **P** —Pending jobs You can use combinations of status options. Separate the options by commas.	**cwcli netshow listjobs -u** *Username* **-p** *Password* **-status** *R,C*
listcmdsets	Displays a list of command sets assigned to the user.	None.	**cwcli netshow listcmdsets -u** *Username* **-p** *Password*
jobresults	Displays results of specified jobs	Specify the job IDs. Separate the job IDs by commas.	**cwcli netshow jobresults -u** *Username* **-p** *Password* **-id** *"Job ID 1" , "Job ID 2" , "Job ID 3"*
help	Displays command usage information.	None.	**cwcli netshow -help**

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for *common_arguments* are described in the following table.

Common Arguments	Description/Action	Usage Notes
`-u` *user*	Enter a valid CiscoWorks username.	None
`-p` *password*	Enter the password for the username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for more details.	None
`[-d` *debug_level*`]`	Set the debug level.	Optional *debug_level* should be a number between 1-5. 1 —The least information is sent to the debug output 5 —The most information is sent to the debug output.
`[-l` *log_filename*`]`	Identifies a file to which Network Show Commands will write log messages. If you do not specify this, the log output will appear on screen.	Optional *log_filename* can be a full path to the file or a filename in the local directory.
`[-m` *Email ID*`]`	Enter your Email ID	You will get the output of the CLI operation in an Email.

Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([]) are optional. Arguments in curly brackets ({}) are required. You must provide one argument from each group of arguments in curly brackets ({}) that is separated by vertical bars (|).

Command Arguments	Description	Usage Notes
Command Arguments for `createjob`		
{**`-device`** *devicelist* | **`-view`** *view_name*}	Defines devices on which you want the command set to run.	*device_list* —List of device names. Separate these names by commas. *view_name* — Name of a device view.

Command Arguments	Description	Usage Notes
{**`-commandset`** *commandset*}	Defines available command sets that you want to run on the selected devices.	*commandset* is the name of the command set that was assigned to you. You can specify more than one command set separated by commas. The command set name is case sensitive. You must specify *command set* or *custom command* or both to create a job.
{**`-customcmd`** *customcommand*}	Defines the user-defined commands that you want to run on the selected devices.	*customcommand* is a user-defined show command. You must specify *command set* or *custom command* or both to create a job. The custom commands which can be run on NetShow are: • **`show`** • **`version`** • **`where`** • **`ping`** • **`traceroute`** • **`?`** You can use the short forms of these commands. For example, **`sh`** for **`show`**.
[**`-description`** *description*]	Gives details of the job.	*description* is a user-defined entry describing the job details.
[{**`-schedule`** *MM/dd/yyyy:HH:mm:ss* **`-scheduletype`** *Once* | *Daily* | *Weekly* | *Monthly* | *LastDayOfMonth* | *6hourly* | *12hourly*}]	You can specify the date and time as well as the frequency of the NetShow job. • To specify the date and time when you want to run the NetShow job, use the schedule option. • To specify the frequency of the job use the scheduletype option. You have to set both the schedule and schedule type options for a scheduled job. You do not have to set the schedule and schedule type for an Immediate job.	*scheduletype* can have any of the following values: • Once • 6hourly • 12hourly • Daily • Weekly • Monthly • LastDayOfMonth If the schedule option is not specified, the job will be created as an immediate job.
[**`-makercomments`** *comments*]	Job creator's comments to Job approver.	
[**`-mkemail`** *email*]	Maker e-mail ID for sending approval notifications	

Command Arguments	Description	Usage Notes
[**`-notificationmail`** *email]*	Defines the e-mail addresses of persons who need to get mails when the job has started and completed.	*email* can contain a comma separated email list. If you do not specify this option in the CLI, the e-mail address specified in the UI are used.
[**`-execution`** *Sequential*|*Parallel*]	Execution policy. Specifies the order in which you want to run the job on the devices. Parallel—Allows the job to run on multiple devices at the same time. By default, the job runs on five devices at a time. Sequential—Allows the job to run on only one device at a time.	If you do not specify these options in the CLI, the corresponding settings from the UI are used.
{**`-primary_user`** *username* **`-primary_pass`** *password*}	Primary username and password to connect to devices.	
{**`-enable_pass`** *password*}	Execution mode password to connect to device.	
[**`-input`** *input file*]	Input file containing the details of the subcommands	If you are specifying the input file, you do not need to specify the subcommands.
Command Argument for `listjob`		
{**`-status`** *status*}	You can specify the status of the job. This can be: • All jobs • Running jobs • Completed jobs • Pending jobs.	
Command Argument for `canceljob`		
{**`-id`** *Job ID*}	You can cancel only one job at a time.	
Command Argument for `deletejob` and `jobdetails`		

Command Arguments	Description	Usage Notes
{`-id` *Job ID, Job ID}*	You can delete more than one job at a time. Enter the Job IDs that you want to delete, separated by commas. You can list the details of more than one job at a time. Enter the Job IDs separated by commas.	
Command Arguments for `jobresults`		
{`-id` *Job ID, Job ID*}	You can list the results of more than one job at a time. Enter the job IDs separated by commas.	
[`-output` *file path*]	You can specify the fully qualified pathname for saving the job results.	If you do not specify this argument, the job results appear in the console itself. If the specified path does not exist, the job results are stored in the default location.

Executing Netshow CLI Remotely

You can execute NetShow CLI from a remote console.

NetShow uses the Remote Access feature in the CLI framework to help you to invoke the NetShow commands from the client in the same way as you run them on the RME server.

The name of the servlet, to be invoked, is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:

  http://*rme-server*:*rme-port*/rme/**cwcli** *payload XML file*

- For GET request:

  http://*rme-server*:*rme-port*/rme/cwcli?command=**cwcli netshow** *command* **-u** *Username* **-p** *Password command_specific_args*

The contents of the payload.xml is:

```
<payload>

   <command>

    cwcli netshow command -u Username -p Password command_specific_args

   </command>

</payload>
```

For example to execute the **listcmdsets** command payload.xml will be as follows:

```
<payload>

<command>

cwcli netshow listcmdsets -u Username -p Password

</command>

</payload>
```

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

Performance Tuning Tool

Performance Tuning Tool (PTT) is a Command Line Interface (CLI) utility that enables you to apply and list various profiles available in CiscoWorks server. Profiles consists of configuration files, which are in the form of XML files whose values are based on the recommendations for various RME applications. For more information on PTT features, refer to PTT Features.

There are two profiles shipped with CiscoWorks. You can use any of the profile that matches the system. For more information on PTT Profiles, see Profiles and PTT.

There maybe multiple configuration files that are involved while applying a profile. The parameters such as, snmp.threads.min, snmp.threads.max, ICSThreadCount, ICS DBConnectionCount, ThreadPoolCount, CDLNumOfThreads, max_db_connections, max_threads_for_config_fetch, EssentialsDMServicesHeapsize,ConfigJobManager.heapsize, and CDA_MIN_THREADS are tuned and available in each profile. You can apply the required profile to the system and improve performance. This is a major advantage of using PTT.

To know more about the command usage, see PTT Commands.

Note Currently, profiles are applicable to RME application only.

PTT Features

The PTT CLI utility allows you to:

- List the profile that is currently applied to the target machine.
- List the profiles that match the system configuration.
- List the profiles that match the operating system.
- Apply a selected profile onto the target machine.
- Reverse the changes done to a target machine by applying the default profile to restore the default settings.
- View details of a profile.

Profiles and PTT

Profiles are XML files whose values are based on the recommendations of the various RME applications. Each profile (XML file) consists of tuned parameters which when applied, improves performance.

There are two profiles that are shipped with LMS 3.0. They are:

- Default Profile
- Perftune - Windows and Perftune - Solaris

Note All the configuration files are backed up before applying a profile.

PTT identifies the matching profile for a CiscoWorks server based on the following criteria:

- The operating system for which the profile is created.
- The System Configurations like Dual CPU and 4 GB RAM.

A profile is considered matching only if it meets these criteria.

When you apply a profile, the tuned parameters, see Table 19-3 corresponding to that profile is applied to the system.

These parameters belong to Sync Archive, Netconfig, Syslog, Device Management, Check Device Attributes (CDA) and Inventory Collection sub systems of the RME application. The profile, with tuned parameters when applied, improves the performance. Before running PTT, ensure that the Daemon manager is stopped

.

Default Profile

A default profile is a profile with default values. It is used to rollback the changes done by PTT. You can roll back the changes made to a profile, by applying the default profile. This action rolls back the parameters to their original values. The parameters and the original values are:

Table 19-3 Default Profile Original Values

RME Sub system	Parameters	Original Values	Platform Supported
CDA	CDA_MIN_THREADS	7	Windows and Solaris
EssentialsDM	ConfigJobManager.heapsize	192m	Windows and Solaris
EssentialsDM	EssentialsDMServiceHeapsize	256	Windows and Solaris
Inventory Collection	snmp.threads.min	10	Windows and Solaris
Inventory Collection	snmp.threads.max	15	Windows and Solaris
Inventory Collection	ICS ThreadCount	10	Windows and Solaris
Inventory Collection	ICS DBConnectionCount	5	Windows and Solaris
NetConfig and SyncArchive	max_threads_for_config_fetch	5	Windows and Solaris
NetConfig and SyncArchive	ThreadPoolCount	10	Windows and Solaris
NetConfig and SyncArchive	CDLNumOfThreads	5	Windows and Solaris
NetConfig and SyncArchive	max_db_connections	20	Windows and Solaris
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for max heap size.)	Xmx	192	Solaris
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for minimum heap size.)	Xms	64	Solaris

Perftune - Windows and Perftune - Solaris

This profile consists of parameters that are tuned to improve performance.

- Perftune - Windows profile is applied to a system that has a Windows operating system, provided the profile matches the required criteria.
- Perftune - Solaris profile is applied to a system that has a Solaris operating system, provided the profile matches the required criteria.

  See Profiles and PTT for more informationon criteria for a profile to match a system.

The parameters that can be tuned are:

Table 19-4 Perftune - Windows and Perftune - Solaris Parameters

RME Sub system	Parameters	Original Values	New Value	Platform Supported
CDA	CDA_MIN_THREADS	7	14	Windows and Solaris
EssentialsDM	ConfigJobManager.heapsize	192m	256	Windows and Solaris
EssentialsDM	EssentialsDMServiceHeapsize	256	512	Windows and Solaris
Inventory Collection	snmp.threads.min	10	20	Windows and Solaris
Inventory Collection	snmp.threads.max	15	25	Windows and Solaris
Inventory Collection	ICS ThreadCount	10	20	Windows and Solaris
Inventory Collection	ICS DBConnectionCount	5	10	Windows and Solaris
NetConfig and SyncArchive	max_threads_for_config_fetch	5	10	Windows and Solaris
NetConfig and SyncArchive	ThreadPoolCount	10	20	Windows and Solaris
NetConfig and SyncArchive	CDLNumOfThreads	5	10	Windows and Solaris
NetConfig and SyncArchive	max_db_connections	20	40	Windows and Solaris
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for max heap size.)	Xmx	192	256	Solaris
Config Management (Config Management Server Daemons - dmgtd.conf Arguments for minimum heap size.)	Xms	64	128	Solaris

Example 1

If the Perftune - Windows profile is applied to a system which already has a default profile applied, the parameters are changed from the original values to new values. See Table 19-4 for Original and New values.

Example 2

If the default profile is applied to a system which already has a Perftune - Windows profile applied to it, the parameters are rolled back to original values. See Table 19-3 for Original values..

PTT Commands

Table 19-5 lists the various PTT command options that you can use. These command options are common for Windows and Solaris.

Table 19-5 PTT Command Options

PTT command options	Description
-apply <*profileName*>	Applies a particular profile. To reset, specify the default profile name as parameter and apply that profile.
-apply	Finds the matching profile and applies it automatically in a single step.
-apply Default	Finds the default profile and applies it automatically in a single step.
-show	Displays the currently applied profile.
-list	Lists all the profiles that match the target operating system.
-list Match	Lists the profile that matches the system configuration.
-view <*profileName*>	Displays the profile details. The details of the profile, which is specified in the command is displayed.
rmeptt -help	Displays help for all commands.

Command Usage

In Windows enter:

```
rmeptt.bat <option> <argument>
```

For example, to list all the profiles that matches the target operating system, the command is:

```
rmeptt.bat -list
```

In Solaris, enter:

```
rmeptt.sh <option> <argument>
```

For example to display the profile details, the command is:

```
rmeptt.sh -view x
```

Where *x* is the name of the profile

.syslogConf.pl Utility

The syslogConf.pl is a perl script CLI utility. You can use this utility to:

- Change Syslog Analyzer Port.
- Change Syslog Collector Port.
- Configure Remote Syslog Collector(RSAC) Address and Port in RME server.
- Change Syslog File Location.

You can run this script in the RME server as well as the RSAC server. All the activities mentioned above can be performed in a RME server by running the syslogConf.pl script from the command prompt.

In RSAC server, you can only change the Syslog Collector Port and Syslog File location. The Syslog Collector and Syslog Analyzer ports can be any number between 1025 and 5000.

This utility is available under:

NMSROOT`/bin/`

A log file for the syslogconf.pl script is available at:

In Solaris

```
/var/adm/CSCOpx/log/SyslogConf.log
```

In Windows

NMSROOT`\log\SyslogConf.log`

Note Before you run the syslogConf.pl script, ensure that the Daemon Manager is stopped.

Running the syslogConf.pl Script

To run the script:

Step 1 Go to the command prompt and enter:

```
NMSROOT/bin/perl NMSROOT/syslogConf.pl
```

When you run this syslogConf.pl script, a message appears with five options.

```
[1] Change Syslog Analyzer Port

[2] Change Syslog Collector Port

[3] Configure Remote Syslog Collector(RSAC) Address and Port

[4] Change Syslog File Location

[Q] Quit

Enter Your Choice:
```

Step 2 Enter your choice.

- If you enter **1** the following message is displayed with the old Syslog Analyser Port number. You are also prompted to enter the new port number for the Syslog Analyser.

  ```
  INFO: You have opted to change Local Syslog Analyser port.

  Old Syslog Analyser Port :xxxx

  Enter new Syslog Analyser port:
  ```

  For example, you can change the Syslog Analyser Port from 4444 to 2222.

  After providing the new port information, the following message is displayed.

  ```
  INFO:Local Syslog Analyser port has been changed from 4444 to 2222 successfully
  ```

- If you enter **2** the following message is displayed with the old Syslog Collector Port number. You are also prompted to enter the new port number for the Syslog Collector.

  ```
  INFO: You have opted to change Local Syslog Collector port.

  Old Syslog Collector Port :xxxx

  Enter new Syslog Collector port:
  ```

  For example you can change the Syslog Collector Port from 1111 to 3333.

  After providing the new port information, the following message is displayed.

  ```
  INFO:Local Syslog Collector port has been changed from 1111 to 3333 successfully
  ```

- If you enter **3**, the following message is displayed, with the old Syslog Collector Port number. You are also prompted to provide the new RSAC Address and the new port number for the Syslog Collector.

  ```
  INFO: You have opted to change RSAC port.
  ```

```
Enter the RSAC Address:
```

```
Old Syslog Collector Port :0
```

```
Enter new Syslog Collector port:
```

Ensure that the RSAC port that you configure in the RME server corresponds with the Collector port configured in the RSAC server.

You can specify srme-w2k as the RSAC Address, and change the Syslog Collector port from 0 to 3456.

After providing the RSAC Address and port information, the following message is displayed.

```
INFO: Remote Syslog Collector(RSAC) port has been changed from 0 to 3456.
```

- If you enter **4**, the following message is displayed with the old Syslog Directory Path. You are also prompted to enter the new Syslog Directory path.

```
INFO: You have opted to change Syslog File Location
```

```
Old Syslog Directory : /var/log/
```

```
Enter Full Path of New Syslog Directory:
```

Ensure that you enter the full directory path, if you are running the syslogConf.pl script on Solaris. You can provide the relative directory path if you are running the syslogConf.pl script on Windows.

For example you can change the Syslog Directory location from /var/log/ to /var/log/newSyslogLoc.

After providing the required information, the following message is displayed.

```
Syslog file location changed from: /var/log/ to: /var/log/newSyslogLoc
```

- If you enter **Q,** you are allowed to quit from the script.

Software Management CLI Utility

You can invoke Software Management (SWIM) features from Command Line Interface (CLI).

The **`cwcli swim`** commands let you use SWIM features from the command line. You can use the **`cwcli swim`** commands to:

- List Images from Software Management (SWIM) Repository
- Export Images from Software Management (SWIM) Repository

These functions are only accessible to the Network Administrator, Network Operator and super users who have all of the roles.

If you do not have permission to run custom commands, you can run a command or command set from the CLI only if:

- The command set is assigned to you by the Administrator.
- The command set has at least one command that can be run on the specified device.

Running cwcli swim Command

The command syntax for running **`cwcli swim`** commands is:

cwcli swim *subcommands common_arguments command_arguments*

In the CLI version, you can provide the arguments in the (operating system shell) command line or in aninput file.

The input file gives you flexibility and control over commands and command sets. You can specify the images on which you want to run the command sets.

In the input file, you can include subcommands and command arguments.

Items in square brackets ([]) are optional; items in curly brackets ({}) are required.

The arguments are described in the following sections.

Subcommands

Subcommands specify the actions that you perform. Valid values for subcommands are described in the following table.

Sub command	Description	Example
listimages	Displays a list of images available in the Software Repository.	**cwcli swim listimages -u** *Userid* **-p** *Password*
exportimages	Exports specified images in a non-compressed format from the Software Repository to any directory. The default target directory is the current directory. For exportimages command either one of these arguments must be mandatorily specified: **-imagenames|-all|-input**	**cwcli swim exportimages -u** *Username* **-p** *Password* [**-imagenames** *imagename1, imagename2...*] [**-all**] [**-dirname** *directoryname*] [**-input** *argumentFile*] [**-m** *email*][**-l** *logfile*]
help	Displays command usage information.	**cwcli swim -help**

Common Arguments

Common arguments specify parameters that apply to all subcommands. Valid values for*common_arguments* are described in the following table.

Common Arguments	Description/Action	Usage Notes
-u *user*	Enter a valid CiscoWorks username.	None
-p *password*	Enter the password for the username. You can also specify the password in a file. See Setting CWCLIFILE Environment Variable for moredetails.	None

[`-l` *log_filename*]	Identifies a file to which Software Management Commands will write log messages. If you do not specify this, the log output will appear on screen.	This argument is optional. *log_filename* can be a full path to the file or a filename in the local directory.
[`-m` *Email ID*]	Enter your Email ID	This argument is optional. You will get the output of the CLI operation in an e-mail.

Command Arguments

Command arguments specify parameters that apply only to specific subcommands. Valid values for command arguments are described in the following table.

Arguments in square brackets ([]) are optional. Arguments in curly brackets ({}) are required. You must provide one argument from each group of arguments in curly brackets ({}) that is separated by vertical bars (|).

Command Arguments	Description	Usage Notes
Command Arguments for `exportimages`		
{`-imagenames` *ImageName1, ImageName2*}	Specify the image names that you want to export using this command.	**`cwcli swim exportimages -u`** *Username* **`-p`** *Password* [**`-imagenames`** *imagename1*, *imagename2*...] [**`-all`**] [**`-dirname`** *directoryname*] [**`-input`** *argumentFile*] [**`-m`** *email*][**`-l`** *logfile*] *ImageName1, ImageName2* —List of images. Separate these names by commas.
{`-all`}	Specify this option if you want to export all images from Software Repository to the current directory or any specified directory.	--

Command Arguments	Description	Usage Notes
{**-input** *argumentFile*}	Input file containing the details of the subcommands	If you are specifying the input file, you need not specify the subcommands. For instance, if you are using sample.txt as the argumentFile for -input command, you have to provide the following command: **cwcli swim exportimages -input** *sample.txt* Example of sample.txt: **-imagenames** {*imagename1}*, [*imagename2...*] **-imagenames** {*imagename4}*, [*imagename5...*] Items in square brackets ([]) are optional; items in curly brackets ({ }) are required.
[**-dirname** *directoryname*]	Specify a directory name if you want to export images to a specified directory using this command.	If you do not specify this the images are exported to the NMSROOT/temp directory, where CLI is launched.

Executing SWIM CLI Remotely

You can execute Software Management (SWIM) CLI from a remote console.

SWIM uses the Remote Access feature in the CLI framework to help you to invoke the SWIM commands from the client in the same way as you run them on the RME server.

The name of the servlet, to be invoked, is /rme/cwcli.

You must invoke the following URLs to run any command.

- For POST request:

  http://*rme-server*:*rme-port*/rme/**cwcli** *payload XML file*

- For GET request:

  http://*rme-server*:*rme-port*/rme/cwcli?command=**cwcli swim** *command* **-u** *Username* **-p** *Password command_specific_args*

The contents of the payload.xml is:

```
<payload>

<command>

cwcli swim command -u Username -p Password command_specific_args

</command>

</payload>
```

For example to execute the **listimages** command payload.xml will be as follows:

```
<payload>
```

```
<command>
cwcli swim listimages -u Username -p Password
</command>
</payload>
```

Note The *Base64* encoded password is used for accessing Software Management (SWIM) CLI remotely.

To invoke the servlet using a script, see the Sample Script to Invoke the Servlet.

The script and the payload file should be residing in the client machine.

CHAPTER 20

Enabling Approval and Approving Jobs Using Job Approval

Resource Manager Essentials (RME) applications, such as NetConfig, Config Editor, Archive Management, and Software Management allow you to schedule jobs to perform their tasks. Job Approval allows you to require that one of a group of users designated as job Approvers approves each job before it can run.

Job Approval sends job requests through e-mail to users on a job's Approver list. If none of the Approvers approve the job before its scheduled run time, or if an Approver rejects the job, the job is moved to the rejected state and will not run.

When Job Approval is enabled, applications that use it, require you to schedule the job to run in the future, rather than immediately. Job approval cannot be enabled for jobs that run immediately.

A user with the appropriate privileges uses a CiscoWorks application to schedule jobs.

When you use Job Approval, different people can perform different tasks:

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform job approval tasks.

Role	**Responsibilities**
System Administrator	Creates and maintains the Approver lists
Approver	Approves/rejects a job, or changes the schedule for a job.

For the new features in this release, see What's New in this Release.

You can select the log level settings for the Job Approval application using the feature Setting System-wide Parameters Using System Preferences (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).

Job Approval is also referred to as Maker Checker in a few places within RME and Common Services. For example, in Loglevel Settings and Permission Report (**Common Services > Server > Reports**) it is mentioned as Maker Checker.

Job Approval Workflow

A typical job approval workflow may look like this:

A system administrator does the following:

1. Specifies user/Approver information (see Specifying Approver Details.)
2. Creates one or more job Approver lists (see Creating and Editing Approver Lists).
3. Assigns Approver lists (see Assigning Approver Lists).
4. Sets up Job Approval (see Setting Up Job Approval).

The planner analyzes the network and prompts the network engineer to schedule a job to perform a needed network change.

The job creator uses a CiscoWorks application to create a job.The application must have an Approver list assigned to it before Job Approval is enabled. Also, it must be scheduled to run in the future (not immediately).

All *Approvers* on the Approver list receive an automatic email notification. The job *Approvers* approve or reject the job (see Approving and Rejecting Jobs) and give their comments.

The job creator and all Approvers on the Approver list receive an automatic e-mail notification.

A job that is not approved or rejected before its scheduled time is automatically moved to the Rejected state. E-mail notification is sent to all Approvers and the user who scheduled the job. If the job is approved, it runs as scheduled.

Specifying Approver Details

Use the option, Approver Details, to maintain information about users with Approver roles.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To specify Approver details:

Step 1 Select **Resource Manager Essentials > Admin > Approval > Approver Details**.

The Approver Details dialog box appears.

Step 2 Click **Synchronize with CommonServices**.

All the approvers in Common Services, with valid E-mail IDs, will appear in the the Approvers list. The E-mails of the approvers will be the same as that added in Common Services.

(You can create a valid CiscoWorks user using the Local User Setup option under **Common Services > Security**).

Whenever an Approver is added to or deleted from Common Services, you should do a synchronize operation, by clicking **Synchronize with CommonServices.**

If you want to change the E-mail ID of any of the Approvers, select the Approver from the Approvers list, and change specifying the new e-mail ID in the E-mail Address field. You can add more than one e-mail, separated by commas

Step 3 Click **Save** to save your changes.

Only those approvers in the ACS mode, who are also approvers in Common Services, are added to RME upon clicking **Synchronize with CommonServices**. All other approvers in ACS, have to be manually added to RME.

To do this, enter the name of the Approver that you want to add in the New Approver field, enter a valid e-mail ID for that user in the E-mail Address field, and click **Save**.

The Approver that you added, appears in the Approvers box.

Creating and Editing Approver Lists

You can use the option Create/Edit Approver Lists to create, edit, or delete Approver lists. Before you create an Approver list, ensure that users have been added, through the Approver Details option (see Specifying Approver Details).

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To create/edit Approvers lists:

Step 1 Select **Resource Manager Essentials > Admin > Approval > Create/Edit Approver Lists**.

The Create/Edit Approver List dialog box appears.

Step 2 Go to the Approver List field and enter a name for an Approver list that you are creating. It can be an alphanumeric name.

Step 3 Click **Add**.

A message appears:

`List` *Listname* `has no users. To save the list successfully, add users and click Save.`

Step 4 Click **OK** to proceed.

The newly-created list appears in the lists box.

(If previously-created lists exist, you can highlight a list to see the List Members in the Users group of fields.)

Step 5 Add users to the newly-created list, by highlighting the list.

In the Users group of fields, the Available Users box lists users who have Approver permissions. Only these users can be added to Approver lists to approve jobs.

- To add a user to the Approver List, select the name from the Available Users list box, and click **Add**.

  The name appears in the List Members list box.

- To remove a user from the Approver list, select the name from the List Members list box, then click **Remove**.

  The name is removed from the List Members list box.

Step 6 Click **Save**.

The Approver Lists box displays the name of the new Approver list and the users on this list appear in the box below Approver Lists.

To edit an Approver List:

a. Select the list.

The approvers of the list appear in the List Members list box.

b. Add new approvers, or remove existing ones in using the Add and Remove buttons in the Users group of fields.

To delete an Approver List:

a. Select the list.

b. Click **Delete**.

A message appears:

```
Are you sure you wish to delete? Approval will be disabled for applications to which
the Listname is assigned!
```

c. Click **OK** to delete the list.

Assigning Approver Lists

You can assign an Approver list to each of the RME applications, from the available Approver lists.

Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To assign an Approver list:

Step 1 Select **Resource Manager Essentials > Admin > Approval > Assign Approver Lists**.

The Assign Approver Lists dialog box appears.

Step 2 Select the required Approver list from the drop-down list box for that application. Repeat this for each of the applications listed here.

Step 3 Click **Assign**.

The selected Approver lists are assigned to the applications.

Setting Up Job Approval

The Approval Policies dialog box allows you to set up Job Approval for all applications for which you can set up job approval. The applications are:

- NetConfig
- NetShow
- Config Editor
- Archive Management. See Using Job Approval for Archive Management for details.

- Software Management. See Using Job Approval for Software Management for details

Prerequisite

Make sure the approver list is assigned to the application, before you enable approval for the application.

Note View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task.

To set up Job Approval:

Step 1 Select **Resource Manager Essentials > Admin > Approval > Approval Policies**.

The Approval Policies dialog box appears. You can enable or disable Job Approval for the following applications:

- NetConfig
- NetShow
- Config Editor
- Archive Management.
- Software Management.

Step 2 Set up Job Approval for the various applications that support job approval, by doing one of the following:

- Select the Enable check box that corresponds to an application, to enable Job Approval.
- Deselect the Enable check box that corresponds to an application, to disable Job Approval.
- Select the All check box to enable Job Approval, for all the applications to which it is applicable.
- Deselect the All check box to disable Job Approval, for all the applications to which it is applicable.

Step 3 Click **Apply** to apply your changes.

After you enable Job Approval, two additional fields appear in the job schedule wizard of the applications. These are:

- Maker Comments—Job creator’s comments.
- Maker E-mail—Job creator’s e-mail address.

Approving and Rejecting Jobs

Use the Approve or Reject Jobs option to approve or reject a job for which you are an Approver. The job will not run until you or another Approver approves it. If no Approver approves the job by its scheduled run time, or an Approver rejects it, the job is moved to the rejected state and will not run.

For periodic jobs, only one instance of the job needs to be approved. If one instance is approved all other instances are considered approved, and vice-versa.

When a job for which you are an Approver is created, you are notified by email.

An Approver can edit the job schedule at the time of approving the job.

The e-mail displays these details:

Details	Description
Job ID	ID of the job that has been put up for approval.
Job Description	Description of the job.
Job Schedule	Date and time for which the job has been scheduled.
Server Name	Name of the server.
Server Time-zone:	Time zone of the server.
Maker Comments	Comments for the Approver, entered by the job creator.
URLS	Two URLs to launch dialog boxes for: • Viewing job details. • Approving or rejecting jobs.

View the Permission Report (**Common Services > Server > Reports**) to check whether you have the required privileges to perform this task. You need to be a user with an Approver role.

Note You will be able to select only those jobs for which you are a part of the Approver List. The other jobs, for which you are not a part of the Approver List, will be disabled.

To approve or reject jobs:

Step 1 Select **Resource Manager Essentials > Job Mgmt > Job Approval**.

The Jobs Pending Approval dialog box appears with the following information about the scheduled jobs on the system:

Column	Description
Job ID	Unique number assigned to the job when it is created. For periodic jobs such as Daily, Weekly, etc., the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click the Job ID hyperlink to view the details of the job.
Owner	Job owner.
Job Type	Application that registered job.
Scheduled to Run at	When job is scheduled to run.
Approver List	Name of Approver list whose members can approve job.
Description	Job description, entered by job creator.

You can filter the pending jobs by any specified criteria using the Filter By drop-down list. Select your criteria and click **Filter**.

Step 2 Either:

- Select the job and click **Approve** to approve the job.

  The job is approved.

Or

- Select **Next**.

  The Job Details dialog box appears (For example, if the ID of the job awaiting approval is 1025, then the title of the dialog box appears as Job Details For Job 1025). You can view/ change the job details before approving or rejecting it.

  The fields in the Job Details box are:

Field	Description
Job	
ID	ID of the job (display only). To see the detailed description of the job, click the View Job Details hyperlink.
Schedule Options	
Run Type	The run type of the job. The Run Types could be any or all of these, depending on the type of the job: • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. To change, select the required run type from the drop-down list.

Field	Description
Current Schedule	
Date	Scheduled date and time of the job. Click **Change Schedule** to change the schedule of the job. You must click the Change Schedule button for the changed schedule to take effect. If you do not click this button, the changed schedule will not be set.
Approver	
Comments	Enter your comments. This field is mandatory only if you are rejecting a job.

Step 3 Click **Approve**.

The job is approved.

If you want to reject the job, enter comments in the Comments text box and then click **Reject**.

Job Management

The Job Management tab of RME allows you to view the status of all RME jobs using the RME Job Browser. See RME Job Browser.

This page also enables you to view all the jobs that are pending approval, and approve or reject them. See Approving and Rejecting Jobs.

You may not be able to use some of these functions if you do not have the required privileges.

RME Job Browser

The RME Job Browser enables you to view the status of all RME Jobs (NetConfig jobs, Device Credential, Archive Management jobs, reports jobs, Inventory collection or polling jobs, purge jobs, etc.).

The job details that you can view here include the job ID, the job type, the job status, the job description, the job owner, the time the job is scheduled to run at, the time of job completion, and the schedule type.

Select **Resource Manager Essentials > Job Mgmt > RME Jobs**.

The RME Job Browser appears.

You can filter the jobs by any specified criteria using the Filter by drop-down list. Select your criteria and click **Filter.**

The fields in the RME Job Browser are:

Column	Description
Job ID	Unique ID of the job. Click on the hyperlink to view the Job details. Some Job IDs have N.x format, which stands for the number of instances of that job. For example, 1003.3 indicates that the Job ID is 1003 and it is the third instance of that job.
Job Type	Type of job. The jobs include, Syslog and Change Audit purge jobs, Device Credential, Inventory collection or polling jobs (system jobs and user-run), NetConfig, Archive Management, or Report jobs.

Column	Description
Status	Status of the job—Scheduled, Successful, Failed, Partial Success, Cancelled, Stopped, Running, Missed Start, Rejected, Approved, Waiting for Approval, Pending, etc.
Description	Description of the job.
Owner	Username of the job creator.
Scheduled At	Date and time at which the job was scheduled.
Completed At	Date and time at which the job was completed.
Schedule Type	Type of job schedule—Immediate, 6- Hourly, 12-Hourly, Once, Daily, Weekly, Monthly, etc. For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

Refresh (Icon)	Click on this icon to refresh the RME Job Browser.

Use the Stop and Delete buttons to stop or delete jobs:

- Stop button—Stops or cancels a running job, or one awaiting approval. You can stop/cancel a running job. You will be asked to confirm the cancellation of the job.

  However, the job is stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state.

- Delete button—Deletes the selected job from the job browser. You can select more than one job to delete. You will be asked to confirm the deletion.

  If the job that you have selected for deletion is a periodic job, then you will be asked to confirm the deletion, as the instances of periodic jobs that are yet to run, would also be deleted.

  You cannot delete a running job.

CHAPTER 21

Setting System-wide Parameters Using System Preferences

You can set system-wide parameters for RME, using the **RME > Admin > System Preferences** tab. Here you can set parameters for RME, such as log level settings, job purge preferences, device attributes and device credentials verification settings.

- Application Log Level Settings
- Job Purge
- RME Device Attributes
- RME Secondary Credentials
- Collection Failure Notification

Application Log Level Settings

You can use this option to set the logging levels for RME packages. You can set the log levels for all RME packages, or at a package (application) level.

Log files are stored at these locations:

- On Windows: *NMSROOT*/log, where *NMSROOT* is the CiscoWorks installation directory.
- On Solaris: /var/adm/CSCOpx/log

To set the log levels:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Application Log level Settings**.

The Set Application Logging Levels dialog box appears.

Step 2 Select the Application from the drop-down list.

Step 3 Select the appropriate log level from the Logging Level drop-down list.

The fields in the Set Application Logging Levels dialog box are:

Application	Module	Description
All	-	Changes the logging level for the entire system.
ArchiveMgmt	• Archive Service • Archive Client	Changes the logging level for Archive Management.
BugToolkit	Bug Toolkit	Changes the logging level for Bug Toolkit.
ChangeAudit	• Change Audit • Change Audit User Interface	Changes the logging level for Change Audit.
CLIFramework	CLI Framework	Changes the logging level for CLI Framework.
ConfigCLI	• Config CLI • Netconfig CLI	Changes the logging level for Config CLI and NetConfig CLI.
ConfigEditor	Config Editor	Changes the logging level for Config Editor.
ConfigJob	Config Jobs	Changes the logging level for Configuration Jobs.
ConfigJobManager	Config Job Manager	Changes the logging level for Configuration Job Browser.
CTMJRrmServer	CTM Jrm Server	Changes the logging level for CTM JRM Server.
CRI	CRI	Changes the logging level for Common reporting Infrastructure.
DeviceManagement	• Device Management Operations • Check Device Attributes	Changes the logging level for Device Management.
DeviceSelector	Device Selector	Changes the logging level for Device Selector.
ICServer	• Inventory Collection Service • Inventory Collection User Interface • Inventory Collection Jobs	Changes the logging level for the IC Server.
Install	• Restore RME CCR • RME PSU Adapter • Migration	Changes the logging level for the Installation modules.
InventoryPoller	Inventory Poller	Changes the logging level for Inventory Poller.
InvReports	Inventory Reports	Changes the logging level for Inventory Reports.
MakerChecker	Maker Checker	Changes the logging level for the Job Approval module.
NCTemplateMgr	NetConfig Template Manager	Changes the logging level for NetConfig Template Manager.
NetConfig	Netconfig Client	Changes the logging level for Netconfig client.

Application	Module	Description
RMECommon	Common RME Functions	Changes the logging level for the common RME functions such as, Job Management tasks, purge tasks, etc.
RMECSTMServer	RME CSTM Server	Changes the logging level for RME CSTM Server.
SoftwareMgmt	• Software Management User Interface • Software Management Jobs	Changes the logging level for the user interface of Software Management and the Software Management job creation workflows.
SyslogAnalyzer	• Syslog Analyzer • Syslog Analyzer User Interface	Changes the logging level for Syslog Analyzer and the user interface of the module.

Step 4 Click **Reset** to apply the default logging levels.

Step 5 Click **Apply** after you set the log levels,

A message appears, that the log levels have been successfully updated.

Job Purge

The Job Purge option provides a centralized location for you to schedule purge operations for the following RME jobs:

- Credential Verification Jobs—Purge all Credential Verification jobs.
- Software Management Jobs—Purge all Software Management jobs such as Image Import, Image Distribution, etc.
- Netconfig Jobs—Purge all NetConfig jobs.
- Archive Management Jobs—Purge Archive Management jobs such as Compliance Check, Deploy Compliance Results, etc.
- Archive Update Jobs—Purge Archive Management collection jobs, *Default config collection job.*
- Archive Poller Jobs—Purge Archive Management polling jobs, *Default config polling job.*
- Archive Purge Jobs—Purge Archive Management purge jobs, *Default archive purge job.*
- Config Editor Jobs—Purge all Config Editor jobs.
- CwConfig Jobs—Purge all cwcli config jobs such as Get Config, Put Config, etc.
- Inventory Collector Jobs—Purge Inventory collection jobs.
- Inventory Poller Jobs—Purge Inventory polling jobs.
- Reports Jobs—Purge all RME Reports jobs
- Reports Archive Jobs—All reports that are archived are purged. You can view all reports that are archived in the Archives window (**Resource Manager Essentials > Reports > Report Archives**).
- NetShow Jobs—Purge all RME NetShow jobs.

You cannot purge the jobs that are in the running state.

The Job Purge contains the following information:

Column	Description
Application	Lists the application for which the purge is applicable.
Status	Whether a purge job is enabled or disabled.
Policy	This value is in days. Data older than the specified value, will be purged. You can change value this as required. This is a mandatory field. The default is 180 days.
Job ID	Unique ID assigned to the job by the system, when the purge job was created. This job ID does not change even when you disable or enable or change the schedule of the purge job. For Purge Now task, job ID is not assigned. Also, if a Job ID already exist for that application, the job ID is not updated for Purge Now tasks. That is, the scheduled purge job is not affected by Purge Now task.
Scheduled At	Date and time that the job was scheduled at. For example: Nov 17 2004 13:25:00.
Schedule Type	Specifies the type of schedule for the purge job: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. (A month comprises 30 days).

You can select the applications by checking the checkboxes next to the application to perform the following tasks using the Job Purge window:

Button	Description
Schedule	Schedule a purge job.
Enable	After you schedule a job, you can enable purge.
Disable	After you schedule a job, if you have enabled the purge job, you can choose to disable it.
Purge Now	Perform immediate purge operation. You can select more than one application to purge jobs corresponding to that application(s) in a single step. After selecting the application(s), click on this button to purge jobs corresponding to that application.

Scheduling a Purge Job

To schedule a purge job:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears.

To create a purge job, select **Schedule**.

The Purge Schedule dialog box appears for the selected application.

Field	Description
Scheduling	
Run Type	Specifies the type of schedule for the purge job: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. (A month comprises 30 days). For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete. For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	1. Click on the date picker icon and select the date, month and year. Your selection appears in the Date field in this format: dd Mmm yyyy (example: 14 Nov 2004). 2. Select the time (hh and mm) from the drop-down lists in the **at** fields.
Job Info	
Days	The default setting for purging archived data is 180 days. That is, data older than 180 days will be purged. You can change this value as required. This is a mandatory field. You can enter non-negative full day only. You cannot enter fractions of days.
Job Description	Based on the option that you selected, you see a default job description. For example, for Software Management purge jobs the default description is: `Purge - Software Management Jobs.` For Reports Archive Purge, the default description is: `Purge - Reports Archive Purge.`

Step 2 Click **Done**.

The purge job appears in the Job Purge dialog box.

Note You cannot purge the jobs that are in the running state.

Enabling a Purge Job

You can enable only a scheduled purge job.

To schedule a purge job, see Scheduling a Purge Job.

To enable a purge job:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears.

Step 2 Click **Enable**.

A confirmation message appears:

```
There is a purge schedule and it is enabled.
```

Step 3 Click **OK**.

The Status column in the Job Purge window displays `Enabled` for the selected application purge job.

Disabling a Purge Job

You can disable only a purge job that is scheduled and enabled.

To schedule a purge job, see Scheduling a Purge Job and to enable a purge job, see Enabling a Purge Job.

To disable a purge job:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears.

Step 2 Click **Disable**.

A confirmation message appears:

```
There is a purge schedule and it is disabled.
```

Step 3 Click **OK**.

The Status column in the Job Purge window displays `Enabled` for the selected application purge job.

Performing an Immediate Purge

Using this option you can purge application jobs immediately. That is, you can purge RME jobs without scheduling and enabling the purge job.

For the Purge Now task, the Job ID is not assigned. Also, if a Job ID already exist for that application, the Job ID is not updated for Purge Now tasks. That is, the scheduled purge job is not affected by Purge Now task.

To perform an immediate purge:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears.

Step 2 Click **Purge Now**.

The Explorer User Prompt dialog box appears.

Step 3 Enter the number of days jobs that have to be purged.

The default setting for purging archived data is 180 days. That is, data older than 180 days will be purged. You can change value this as required.

You can enter non-negative full day values only. You cannot enter fractions of days.

Step 4 Click **OK**.

The Purge Job Details window appears displaying the purged job details.

Note You cannot purge the jobs that are in the running state.

RME Device Attributes

This option enables you to set the default values for device attributes. These values are applicable to all devices in RME. The RME device attributes are:

- SNMP Retry—Number of times that the system should try to access devices with SNMP options.

  The default value is 2. The minimum value is zero and the maximum value is 6.
- SNMP Timeout—Amount of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 2 seconds and the minimum value is zero seconds. There is no maximum value limit. Changing the SNMP timeout value affects inventory collection.
- Telnet Timeout—Amount of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 36 seconds and the minimum value is zero seconds. There is no maximum value limit.

  Changing the telnet timeout value affects inventory collection.
- Natted RME IP Address—The RME server ID. This is the translated address of RME server as seen from the network where the device resides.

  You need to enable support for NAT, in a scenario where RME tries to contact devices outside the NAT boundary.

  The default value is Not Available.
- TFTP Timeout—Amount of time that the system should wait for a device to respond before it tries to access it again.

  The default value is 5 and the minimum value is 0 seconds. There is no maximum value limit.

To edit the RME device attributes:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > RME Device Attributes**.

The RME Device Attributes dialog box appears.

Step 2 Enter the default values for:

- SNMP Retry
- SNMP Timeout
- Telnet Timeout
- Natted RME IP Address

- TFTP Timeout

The value you enter here will be applicable for all RME devices. You can change the value for individual devices and also enter the device serial number information using the Edit Devices Attributes option on RME Devices window. (see To set or edit the RME device attributes for a single RME device.)

Step 3 Click **Apply**.

A confirmation message appears:

```
Default settings are updated successfully.
```

Step 4 Click **OK**.

RME Secondary Credentials

The RME server polls and receives two types of credentials from each device and populates the Device Credential Repository (DCR).These credentials are:

- Primary Credentials
- Secondary Credentials

RME uses either the primary or secondary credentials to access the devices using the following protocols:

- Telnet
- SSH

The RME server first uses the Primary Credentials to access the device. The Primary Credentials is tried out three times and on failure the Secondary Credentials is tried out three times. Secondary Credentials is used as a fallback mechanism in RME 4.1 for connecting to devices. For instance, if the AAA Server is down, accessing devices using their primary credentials will lead to failure.

You can add or edit the Secondary Credentials information through the DCR page available in CiscoWorks Common Services if the Secondary Credential information is not available for a device.

Note The use of Secondary Credentials fallback is applicable for both Login and Enable connectivity.

You can use the RME Secondary Credential dialog box to enable or disable Secondary Credentials fallback when the Primary Credentials for a device fails. This is a global option which you can use to enable or disable the use of Secondary Credential fallback for all RME applications.

To enable or disable the Secondary Credentials fallback:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > RME Secondary Credentials**

The RME Secondary Credentials dialog box appears.

Step 2 Do either of the following:

- Check **Fallback to Secondary Credentials** checkbox if you want to enable the Secondary Credential fallback.

Or

- Uncheck **Fallback to Secondary Credentials** checkbox if you want to disable the Secondary Credential fallback.

Step 3 Click either **Apply** to apply the option or click **Cancel** to discard the changes.

Collection Failure Notification

You can use the Collection Failure Notification window to configure the receipt of Trap messages by the host(s) mentioned in the env.properties file on Inventory Collection or Config Fetch failure. This Trap is sent for each device from the RME server whenever the collection does not happen.

The destination IP address to which the traps are to be sent can be configured in the env.properties file. This file is available under this location:

NMSROOT`/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/util/env.properties`

where *NMSROOT* is the actual CiscoWorks install directory.

The variables that can be configured in the env.properties file are:

NOTIFY_IP

This variable allows you to configure the destination IP addresses for the receipt of trap messages. The initial value assigned to this variable is *DEFAULT*. Replace this DEFAULT with the IP address of the host(s) to which the Trap messages need to be sent. You can specify comma-separated IP addresses to which the trap messages are to be sent.

Example 1

You can set 10.10.10.10 as the destination IP Address to receive trap messages.

```
NOTIFY_IP = 10.10.10.10
```

Example 2

You can set 10.10.10.10, 20.20.20.20, and 30.30.30.30 as the destination IP Addresses to receive trap messages.

```
NOTIFY_IP = 10.10.10.10,20.20.20.20,30.30.30.30
```

NOTIFY_PORT

This variable allows you to configure the destination Port number to which the trap messages are to be sent. The initial value assigned to this variable is 162 and it is the default value. You can change this port number if you want to assign anyother port to receive Trap messages. Trap 162 is the recommended port to receive trap messages.

Example

You can set port 164 as the destination Port to receive the trap messages.

```
NOTIFY_PORT = 164
```

Any third party Trap receivers in the host(s) mentioned in the env.properties can receive the Trap messages on Config collection/Inventory collection failure.

Table 21-1 lists the various options available in the Collection Failure Notification Window:

Table 21-1 Notification on Failure

Field	**Description**
Config Collection	Check this option, if you require the Config Fetch Failure Trap notification to be sent to the host(s) mentioned in the env.properties file. Uncheck this option if you do not want the Config Fetch Failure trap notification to be sent to the host(s) mentioned in the env.properties file.
Inventory Collection	Check this option, if you require the Inventory Collection Failure trap notification to be sent to the host(s) mentioned in the env.properties file. Uncheck this option if you do not want the Inventory Collection Failure Trap notification to be sent to the host(s) mentioned in the env.properties file.
All	Check this option, if you require both the Config Fetch Failure and Inventory Collection Failure trap notifications to be sent to the host(s) mentioned in the env.properties file.
Apply	Click to accept the changes made.

Configuring Trap Notification Messages

To configure the distribution of trap notification messages from RME to the connected hosts:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Collection Failure Notification**

The Notification on Failure dialog box appears. See Table 21-1 to further complete the selection in this dialog box.

Step 2 Click **Apply** to accept the changes made.

Examples for Collection Failure Notification

Example for Config Collection Trap Notification

For example, assume you enable the Config Fetch option. By enabling this option you allow trap notifications to be sent to the host(s) mentioned in the env.properties file.

After that you add few new devices to RME and schedule a job to fetch the configurations for all the devices. If there is a Config Fetch Failure because the scheduled job cannot fetch the configurations for the new devices, the trap notification is sent to the host(s) mentioned in the env.properties file for each Config Fetch Failure and for each device.

Example for Inventory Collection Trap Notification

For example, assume you enable the Inventory Collection option. By enabling this option you allow trap notifications to be sent to the host(s) mentioned in the env.properties file on Inventory Collection Failure to the specified port.

After that you add few new devices to RME and schedule a job to fetch the inventory information for all devices. If there is a Inventory Collection Failure because the scheduled job cannot fetch the inventory details for the new devices, the trap notification is sent to the host(s) mentioned in the env.properties file for each Inventory Collection Failure and for each device.

Fields in a Trap Notification Message

Table 21-2 lists the various fields that constitute a Configuration Fetch or Inventory Collection Failure trap notification message.

Table 21-2 Fields in a Trap Notification Message

Field	**Description**
Application Name	RME application that caused this change or identified the change and generated the notification.
Device Display Name	Network device for which the inventory or configuration collection has failed.
Collection Failure Time	Time at which the inventory or configuration collection job failed.

Error Message	The message that describes the reason for the collection failure. Some examples of trap error messages:
	`Inventory Collection Failed due to SNMP TimeOut Exception.`
	`Config Collection Failed due to authentication failure.`

APPENDIX A

RME Troubleshooting Tips and FAQs

This Appendix covers the Troubleshooting tips and FAQs for:

- Device Management
- Inventory
- Inventory Reports
- Archive Management
- NetConfig
- Config Editor
- Software Management
- Syslog Analyzer and Collector
- Job Approval
- Bug Toolkit
- cwcli config
- cwcli export
- NetShow
- Administration
- Contract Connection

For other Installation related FAQs and Troubleshooting tips, see the *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0*

Device Management

This section provides troubleshooting information and FAQs for the Device Management application:

- Device Management FAQs
- Troubleshooting Device Management:

Device Management FAQs

- Q.Can we add or import devices directly to RME?
- Q.How can I verify that the Device Credentials configured on the device match those in the RME inventory?

- Q.How do I edit the device credentials in RME?
- Q.How can I check the device credentials while adding the devices to RME?
- Q.What are device credentials and RME device attributes?
- Q.How are the device credentials mapped in Device and Credential Repository?
- Q.What happens when I delete a device in RME?
- Q.What are the most frequent causes of device import failures?
- Q.How do I increase the SNMP Timeout and Telnet Timeout values for RME devices?

Q. Can we add or import devices directly to RME?

A. No, you cannot add or import devices directly to RME. You have to first add or import devices to Device and Credential Repository (DCR) (**Common Services > Device and Credentials > Device Management**).

If the Automatically Manage Devices from Credential Repository option is enabled in the Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**), then the devices are added automatically to RME. By default, this option is enabled.

If this option is disabled, then you have to add devices to RME manually from RME Devices window (**Resource Manager Essentials > Devices Device Management RME Devices**).

Q. How can I verify that the Device Credentials configured on the device match those in the RME inventory?

A. Click on the View Credential Verification Report in the Device Credential Verification (**Devices > Device Management > Device Credential Verification**) dialog box:

- If you have already selected the credentials that have to be verified then the Credential Verification Report appears.
- If you have not selected the credentials that have to be verified, then a message appears:

```
None of the devices have credential verification data. Click Check Device
Credential to select the credentials that have to be verified and then click
Credential Verification.
```

See Using Device Credential Verification Window section in Chapter 3: *Adding and Troubleshooting Devices Using Device Management of the User Guide for Resource Manager Essentials 4.1* for more information at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_list.html

Q. How do I edit the device credentials in RME?

A. You can edit the credentials either in:

- Common Services (**Common Services > Device and Credentials > Device Management > Edit** (button)

  or

- RME (**Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Edit Device Credentials** (button))

Q. How can I check the device credentials while adding the devices to RME?

A. To check the device credentials while adding devices to RME, you have to enable the Verify Device Credentials While Adding Devices option in the Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**).

You can select the device credentials that have to be verified in the Device Credential Verification Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Credential Verification Settings**).

Q. What are device credentials and RME device attributes?

A. The following are the device credentials:

- SNMP Read Community String
- SNMP Write Community String
- SNMPv3
- Telnet
- Telnet Enable Mode User Name and Password
- SSH
- SSH Enable Mode User Name and Password

The following are the RME device attributes:

- Serial Number
- SNMP Retry
- SNMP Timeout
- Telnet Timeout
- RME ID (NAT ID)

Q. How are the device credentials mapped in Device and Credential Repository?

A. The following table describes the mapping of device credentials in Device and Credential Repository:

Device Credentials	Device and Credential Repository
Telnet password	primary_password
Enable password	primary_enable_password
Enable secret	primary_enable_password
Tacacs username	primary_username
Tacacs password	primary_password
Tacacs enable username	Not used in CSV 3.0
Tacacs enable password	primary_enable_password
Local username	primary_username
Local password	primary_password

The order of preference to set these values in Device and Credential Repository is:

- If Tacacs username, password, enable password is set, then these values will be set as primary_username, primary_password and primary_enable_password.

- If Local username and password is set, then the values will be set as primary_username and primary_password.
- If Telnet password, Enable Password, and Enable Secret are set, then the values will be set as primary_password, and primary_enable_password (for both Enable Password, and Enable Secret).

Q. What happens when I delete a device in RME?

A. When you delete a device in RME, all RME data related to that particular device is deleted.

However, the device data is still available in the Device and Credential Repository. You can re-add the devices into RME using RME Devices window (**Resource Manager Essentials > Devices > Device Management > RME Devices > Add Devices**).

Q. What are the most frequent causes of device import failures?

If after importing a device, it remains in the Pre-deployed state, to troubleshoot, see Diagnosing Pre-deployed Devices under Chapter 3: Adding and Troubleshooting Devices Using Device Management of the *User Guide for Resource Manager Essentials 4.1* for more information at this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_list.html

For more about RME device states, see User Guide for Resource Manager Essentials 4.1:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_list.html

Q. How do I increase the SNMP Timeout and Telnet Timeout values for RME devices?

A. You can edit the RME device attributes using either of these options:

- Set a default device attributes value for all RME devices using **Resource Manager Essentials > Admin > System Preferences > RME Device Attributes**.

  Or
- Set different device attributes value for different RME devices using **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes**.

See Editing RME Device Attributes section under Chapter 3: Adding and Troubleshooting Devices Using Device Management of the *User Guide for Resource Manager Essentials 4.1* for more information at this URL:

http://www.cisco.com/en/US/products/sw/cascara/ps2073/products_user_guide_list.html

Troubleshooting Device Management:

Message ID	Error Message	Probable Cause	Possible Action
DM0001	Select a Normal device and click this option.	You have not selected a Normal device before performing the action	Select a Normal device and perform the action.
DM0003	This software has a RESTRICTED license for managing a limited number of devices. Click here <a href=/cwhp/maas.licenseInfo.do target=_blank> for current licensing information. Contact your Cisco representative to determine if additional licenses can be purchased for this server.	Software has a restricted license to manage a limited number of devices	Purchase additional license and perform the action
DM0004	File name should be between 1 and 255 characters	The file name given for Export or Import either has no characters or more than 255 characters	Enter a file name between 1 and 255 characters.
DM0005	Either you have not selected a valid file or the file does not have required permission	The file selected for Export or Import does not have the required permissions for Read/Write.	Modify the file permissions to get Read/Write permisions.
DM0006	Selected file name is invalid or blank.	You have not selected a file for Export.	Select a file and perform the action
DM0007	Attribute values for devices are invalid. See EssentialsDM.log for more details.	You have entered invalid values for some attributes while importing attributes for devices.	Enter valid values for the attributes and perform the task.
DM0008	There are no new devices in DCR. Add new devices to DCR and continue with this flow.	All devices in DCR are already managed by RME. There are no new devices to be managed.	Add some more devices in DCR and perform the task.
DM0009	Either you have not entered a valid filename or the file does not exist.	The filename that you entered for Import task either does not exist or does not have Read permission.	Enter a valid filename and perform the task.

Inventory

This section provides the troubleshooting information and FAQs for the Inventory application:

- Inventory FAQs

- Troubleshooting Inventory

Inventory FAQs

- Q.Where can I find out what devices are supported by RME Inventory?
- Q.What are the main methods that I have for performing data collection?
- Q.What does the Inventory Poller do?
- Q.How do I know when a schedule collection was last performed and how long it took?
- Q.How can I see the most recent changes?
- Q.Where can I find out what devices are supported by RME Inventory?
- Q.Why is the Device Serial Number field blank in Inventory?
- Q.How can I make sure a device's serial number is correct, and fix it, if it is wrong?
- Q.Why am I receiving an error message, `Write Community = INCORRECT` although I have entered the correct Write Community String?
- Q.What do I need to collect from my Solaris or Windows machine when troubleshooting RME Inventory?
- Q.Is there an option to disable/enable Secondary Credentials fallback in RME?
- Q.How can I generate an End of Sale / End of Life Report?
- Q.How can I generate a PSIRT Summary Report?
- Q.How can I change the Cisco.com Fetch interval for End of Sale/End of Life report and PSIRT reports?
- Q.What is the prerequisite to generate the PSIRT/End of Sale End of Life reports?
- Q.Is it possible to generate PSIRT Summary report for all categories of devices?
- Q.Why are there multiple End of Sale/End of Life announcements for a device?
- Q.Is it possible to schedule an Immediate PSIRT Summary or End of Sale/End of Life report job?

Q. Where can I find out what devices are supported by RME Inventory?

A. You can find out what devices are supported by RME Inventory in any one of the following ways:

- Check the Supported Device Table on Cisco.com to see whether or not an upgrade to RME is required.

  Or

- Follow this procedure:

  a. Select **CiscoWorks Common Services > Software Center > Device Update**.

     The Device Updates dialog box appears.

  b. Click **Resource Manager Essentials**.

     The Package Map dialog box appears with the list of supported devices.

  Or

- In the RME Device Selector if the device is grayed out, it means that RME does not support the device.

Q. What are the main methods that I have for performing data collection?

A. At the time of RME installation, system jobs are created for both Inventory collection and polling with their own default schedules. A periodic inventory collection job collects inventory data from all managed devices and updates your inventory database.

Similarly, the periodic polling polls devices and updates the inventory database. You can change the schedule of these default, periodic system jobs (**Resource Manager Essentials > Admin > Inventory > System Job Schedule**).

System Inventory Collection is the heavyweight collection method. It collects all managed devices at a scheduled time and updates the database. You can view Inventory Collection status at **Resource Manager Essentials > Devices > Inventory > View Inventory Collection Status.**

You can also create and run an Inventory Collection job on selected devices by creating a job (**Resource Manager Essentials > Devices > Inventory > Inventory Jobs**. In the Inventory Job Browser that appears, click **Create**. For details on how to create a job, see *User Guide for Resource Manager Essentials 4.1*).

Q. What does the Inventory Poller do?

A. The Inventory Poller uses a "lightweight" mechanism to determine whether database information is out-of-date. Although the Inventory Poller itself does not perform an actual collection, it determines whether any device information is out-of-date. If information is outdated, the Inventory Poller initiates a full collection on the pertinent devices.

Q. How do I know when a schedule collection was last performed and how long it took?

A. In the Inventory Job Browser (**Resource Manager Essentials > Devices > Inventory > Inventory Jobs**) click on the Job ID for a specified job. The Job Details dialog box appears. You can view the complete details of the inventory collection here, by browsing through the left navigation pane.

At a high level, you can view Inventory Collection status at **Resource Manager Essentials > Devices > Inventory > View Inventory Collection Status**.

Q. How can I see the most recent changes?

A. To view inventory changes made in the last 24 hours, use the 24 Hour Inventory Change Report option:

a. Select **Resource Manager Essentials > Reports > Report Generator**.

   The Report Generator dialog box appears.

b. From the first drop-down list, select the Inventory application.

c. From the second drop-down list, select 24 Hour Inventory Change Report.

   The Inventory Change Report dialog box appears.

d. Select the devices, using the Device Selector, and leave the Run Type as Immediate.

e. Click **Finish**.

   The 24 Hour Inventory Change Report appears.

To view changes made since the last scheduled collection, use the Change Audit application.

Q. Why is the Device Serial Number field blank in Inventory?

A. The field is blank because inventory could not obtain the information from the device. This is caused by one of these reasons:

- The serial number was not set in the device software when the device was introduced to the network. This should have been done using CLI, as described in the device configuration guide.

- The device does not support MIBs for serial numbers.

In either case, you can set the serial number in the inventory database in this way:

a. Select **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes**.

The Device Attributes Information dialog box appears.

b. Select the device and enter the correct serial number printed on the device chassis, in the RME ID field and click **Modify**.

Q. How can I make sure a device's serial number is correct, and fix it, if it is wrong?

The serial number in inventory should always match the number printed on the chassis. If the serial number does not match the number on the chassis, you can change it in this way:

a. Select **Resource Manager Essentials > Devices > Device Management > RME Devices > Edit Device Attributes**.

The Device Attributes Information dialog box appears.

b. Select the device and enter the correct serial number printed on the device chassis, in the RME ID field and click **Modify**.

Q. Why am I receiving an error message, **`Write Community = INCORRECT`** although I have entered the correct Write Community String?

A. Check whether you have dropped the system group from the view (read-view and write-view). The system group must be available for Read and Write task. In MIB-II, the system group is available as the default.

Q. What do I need to collect from my Solaris or Windows machine when troubleshooting RME Inventory?

A. You can collect troubleshooting information about the status of the server using the Collect Server Information option in Common Services:

a. Login as Administrator.

b. Select **Common Services > Server > Admin > Collect Server Information**.

The Collect Server Information dialog box appears.

c. Click **Create**.

A list of report modules and options are displayed.

d. Select the modules you want to include and click **OK**.

By default, all the modules are selected.

If you collect server information using the Collect Server Information GUI option the data is stored in /opt/CSCOpx/htdocs/collect.

A command line script is also available at /opt/CSCOpx/bin/collect.info. The command script outputs data to STDOUT. For more details on the command script, see the User Guide.

For both Windows and Solaris, you can turn on the debug for ICServer and other processes from the GUI.

You can use the LogLevel Settings option to set the logging levels for RME packages. You can set the log levels for all RME packages, or at a package (application) level.

To set the log levels:

a. Select **Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**.

   The Set Application Logging Levels dialog box appears.

b. Select the application from the drop-down list.

c. Select the appropriate log level from the Logging Level drop-down list.

d. Click **Default** to apply the default logging levels.

e. After you set the log levels, click **Apply**.

   A message appears, that the log levels have been successfully updated.

Log files are stored at these locations:

On Windows: *NMSROOT*/log, where NMSROOT is the CiscoWorks installation directory.

On Solaris: /var/adm/CSCOpx/log

You need to collect the following log files:

On Windows:

- IC_Server.log
- EssentialsDM_Server.log
- EssentialsDM.log
- ICServer.log
- ICServer_UI.log
- InvReports.log

Job-specific log files that you need are at these locations:

- *NMSROOT*\files\rme\jobs\InvPoller
- *NMSROOT*\files\rme\jobs\Inventory
- *NMSROOT*\files\rme\jobs\ICServer

On Solaris:

- daemons.log
- EssentialsDM_Server.log
- IC_Server.log

Job-specific log files that you need are at these locations:

- /var/adm/CSCOpx/files/rme/jobs/ICServer
- /var/adm/CSCOpx/files/rme/jobs/InvPoller
- /var/adm/CSCOpx/files/rme/jobs/inventory

You can then e-mail these debug log files along with the Collect Server Info output, to Cisco TAC.

Q. Is there an option to disable/enable Secondary Credentials fallback in RME?

A. You can Enable or Disable fallback to Secondary Credentials by following the steps below:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > RME Secondary Credentials**

The RME Secondary Credentials dialog box appears.

Step 2 Do either of the following:

- Check the **Fallback to Secondary Credentials** checkbox if you want to enable the Secondary Credential fallback.

Or

- Uncheck the **Fallback to Secondary Credentials** checkbox if you want to disable the Secondary Credential fallback.

Step 3 Click either **Apply** to apply the option or click **Cancel** to discard the changes.

Q. How can I generate an End of Sale / End of Life Report?

A. To generate End of Sale / End of Life Report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, and select **Inventory**.

Step 3 Go to the second drop-down list box, select the **End of Sale / End of Life Report**.

Step 4 Select the required devices using the Device Selector.

Step 5 Enter the required information to generate the required report.

Q. How can I generate a PSIRT Summary Report?

A. To generate a PSIRT Summary Report:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Reports dialog box appears, in the Report Generator page.

Step 2 Go to the first drop-down list box, and select **Inventory**.

Step 3 Go to the second drop-down list box, select the **PSIRT Summary Report**.

Step 4 Select the required devices using the Device Selector.

Step 5 Enter the required information to generate the required report.

Q. How can I change the Cisco.com Fetch interval for End of Sale/End of Life report and PSIRT reports?

A. To update the Cisco.com Fetch interval:

Step 1 Go to **Resource Manager Essentials > Admin > Inventory > Cisco.com Fetch Interval**.

Step 2 Select a frequency at which you require the PSIRT information to be retrieved from Cisco.com.

The duration can be 1 hour or 3 hours or 24 hours or 7 days or 30 days. The default value is 24 hours.

Step 3 Select a frequency at which you require the EoSale/EoL information to be retrieved from Cisco.com.

The duration can be 1 hour or 3 hours or 24 hours or 7 days or 30 days. The default value is 7 days.

Step 4 Click **Save** to save the changes to the frequencies.

Q. **What is the prerequisite to generate the PSIRT/End of Sale End of Life reports?**

A. Ensure that Inventory collection for devices has taken place before you generate a PSIRT/End of Sale End of Life report.

Q. Is it possible to generate PSIRT Summary report for all categories of devices?

A. The PSIRT Summary report displays the PSIRTs only for Cisco IOS device categories.

Q. Why are there multiple End of Sale/End of Life announcements for a device?

A. A device consists of many components. Each component is subject to End of Sale/End of Life. So there maybe multiple End of Sale/End of Life announcements for a device.

Q. Is it possible to schedule an Immediate PSIRT Summary or End of Sale/End of Life report job?

A. Yes. You can schedule an Immediate PSIRT Summary or End of Sale/End of Life report job. You can use the Cisco.com Fetch Interval option to configure the interval at which the PSIRT and End of Sale/End of Life announcements are retrieved from Cisco.com.

However, there maybe delays upto 3 hours as the announcements are refreshed in the Cisco servers every 3 hours. So the information that is represented in the Immediate PSIRT Summary report or End of Sale/End of Life report is 3 hours old.

Troubleshooting Inventory

This section provides the troubleshooting information for the Inventory application:

Message ID	Error Message	Probable Cause	Possible Action
ICSU0001	Could not create database connection.	Could not create database connection. RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0002	Could not create JRM interface object.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0003	Could not create job.	Unknown exception occured.	Retry after sometime. If the problem persists, contact Cisco TAC.
ICSU0004	Could not display Job Details.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0005	Could not display Job Details.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC

Message ID	Error Message	Probable Cause	Possible Action
ICSU0006	Could not get device support information.	Device packages may not be installed.	Check whether the device packages have been completely installed. If the problem persists, contact Cisco TAC.
ICSU0007	Could not create job.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0008	Could not create job.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0009	Could not display job settings for editing.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0010	Could not display job settings for editing.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0011	Could not display job settings for editing.	Unknown error occured.	Retry after sometime. If the problem persists, contact Cisco TAC.
ICSU0012	Could not edit job.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0013	Could not edit job.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0014	Could not edit job.	Unknown error occured.	Retry after sometime. If the problem persists, contact Cisco TAC.
ICSU0015	Could not stop job.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0016	Could not delete job.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.

Message ID	Error Message	Probable Cause	Possible Action
ICSU0017	Could not display job browser entries.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. Also make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0018	Could not filter based on given options.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0019	Could not filter based on given options.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0020	Could not filter based on given options.	Could not communicate with JRM or with RME DB Service. Jrm/CTMJrmServer or RME DB Service may be down.	Make sure that Jrm/CTMJrmServer is running. Also make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0021	Could not show summary.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSU0022	Could not get the Inventory Last Collected Time.	Inventory may not be collected at least once.	Try to collect Inventory for this device and try this task after the Inventory Collection. If the problem persists, contact Cisco TAC.
ICSU0023	Could not stop job.	Could not communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSU0024	Could not work with Resource Manager Essentials Database.	EssentialsDBEngine and/or RMEDbMonitor may be down.	Make sure that EssentialsDBEngine/ RMEDbMonitor is running. Check the log file for more details. If the problem persists, contact Cisco TAC.
ICSU0025	Could not work with Job Resource Manager.	Jrm and/or CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. Check the log file for more details. If the problem persists, contact Cisco TAC.

Message ID	Error Message	Probable Cause	Possible Action
ICSJ0001	Could not create database connection.	RME DB Service may be down.	Make sure that RME DB Service is running. If the problem persists, contact Cisco TAC.
ICSJ0002	Could not run job.	Cannot communicate with JRM. Jrm/CTMJrmServer may be down.	Make sure that Jrm/CTMJrmServer is running. If the problem persists, contact Cisco TAC.
ICSJ0003	Could not run the job.	Job ID passed by Jrm is null.	Restart Jrm. If the problem persists, contact Cisco TAC.
ICSJ0004	Could not run job.	Invalid license.	Obtain a valid License.
ICSJ0005	Could not create log file.	There is already a file with the same name as the directory to be created.	Delete the file with the same name as the directory to be created.
ICSJ0006	Could not create log file.	There is already a file with the same name as the Job ID.	Delete the file with the same name as the Job ID.
ICSJ0007	Could not run the job.	Could not create CSTM Server	Retry after some time. If the problem persists, restart Daemon Manager. If the problem persists, contact Cisco TAC.
ICSJ0008	Request to collect inventory failed.	ICServer may be down.	Start the ICServer and try again. If the problem persists, contact Cisco TAC.
ICSJ0009	Could not send e-mail.	SMTP Server may be down	Check the SNMP server. If the problem persists, contact Cisco TAC.
ICSJ0010	Could not send e-mail.	No SMTP Server configured.	Configure the SMTP Server and try again. If the problem persists, contact Cisco TAC.
ICSJ0011	Could not access DCR Server	The user is not authorized to perform the task.	Check the role of the user.
ICSJ0012	Could not establish connection to Daemon Manager.	Unknown error while connecting to Daemon Manager.	Restart Daemon Manager. If the problem persists, contact Cisco TAC.
ICSJ0013	Could not send OK Signal to Daemon Manager.	Unknown error while connecting to Daemon Manager.	Restart Daemon Manager. If the problem persists, contact Cisco TAC.
ICSJ0014	Could not run job.	Error while running the job framework	Retry after some time. If the problem persists, contact Cisco TAC.

Message ID	Error Message	Probable Cause	Possible Action
ICSJ0015	Could not run the job.	CSTM error while publishing the URN.	Retry after some time. If the problem persists, restart Daemon Manager. If the problem persists, contact Cisco TAC.
ICSJ0016	Exception while running the job.	Error occured while receiving the message through the Event Sub-system.	Retry after some time. If the problem persists, restart Daemon Manager. If the problem persists, contact Cisco TAC.
RICS0001	Cannot successfully collect Inventory Information for the device.	Internal Error	Try Collecting Inventory for the device again. If the problem persists, in the log directory look for IC_Server.log. If you search for the Device IP, you will see an exception trace. Contact Cisco TAC with these details.
ICSJ0017	Cannot run more than 33 concurrent jobs in RME.	More than 33 jobs running concurrently in RME.	$*NMSROOT*\CSCOpx\MDC\tomcat\webapps\rme\WEB-INF\lib\ctm_config.txt has MAX_VM_PORTS set by default to 40. Increase this if you want more than 33 concurrent jobs.

Inventory Reports

This section provides the troubleshooting information for the Inventory Reports application:

Message ID	Error Message	Probable Cause	Possible Action
INVREP0002	You have not updated the template.	Either the database may not be running or there may be other database related problems.	Check the invreports.log for more details. Make sure that RMEDbEngine service is running.
INVREP0003	You have not created the template.	Either the database may not be running or there may be other database related problems.	Check the invreports.log for more details. Make sure RMEDbEngine service is running.
INVREP0007	The Query building task failed.	Either there is a problem in the building join conditions or the database may not be running	Check the invreports.log for more details. Verify the generated queries in the log generated in debug mode.
INVREP0008	Report generation failed.	The template may have been deleted from another browser or by another user.	Check the Custom templates screen for this template. If it is not there, create it.

Message ID	Error Message	Probable Cause	Possible Action
INVREP0009	Report generation failed.	One of the UDFs given in the template might have modified or deleted.	Check the invreports.log for modified or deleted UDF details and redefine the template. • If the UDF has been modified, modify the corresponding rule accordingly. • If UDF has been deleted, delete the corresponding rule from template.
INVREP0013	Could not create file with the name *filename*	You may not have permissions to create a new file in the current folder.	Check the permissions. Check the invreports.log for more details.
INVREP0015	Report generation failed. Could not get device ids from Device and Credential Repository (DCR)	The DCR server may not be running	Check the log for more details. Make sure the DCR Server is running.
INVREP0016	Could not generate CSV File -%1.	You may not have permissions to create a new file in the current folder.	Check the permissions. Check the invreports.log for more details.
INVREP0017	Reports generation partially succeeded.	You have attempted to run many commands from a file. Some of the commands have failed.	1. Check the invreports.log 2. Execute the same command with the **–log** option 3. See the corresponding log for more details.
INVREP0021	Error occured while generating report.	Unknown error.	Check the invreports.log for more details.
INVREP0022	Data not available or the database connection failed.	Check whether the RME database is running.	If the database engine is not running start the engine and try again.
INVREP0023	Job creation failed.	JRM Server may not be running.	1. Check the status of JRMServer using the pdshow jrm command 2. Start JRM and try creating the job
INVREP0028	Could not get database connection.	Check whether the RME database is running.	If the database engine is not running start the engine and try again.
INVREP0025	Job creation failed.	The JRM Server may not be running.	Start JRM and try creating the job
INVREP0026	Could not get data from the database.	Check whether the RME database is running.	1. Check the status of JRMServer using the pdshow jrm command 2. Start JRM and try creating the job If the database engine is not running start the engine and try again.

Message ID	Error Message	Probable Cause	Possible Action
INVREP0027	Database connection resource release failed.	Check whether the RME database is running.	If the database engine is not running start the engine and try again.
INVREP0028	Could not update the database.	Check whether the RME database is running.	If the database engine is not running start the engine and try again.
INVREP0029	Could not find the selected archive in the database.	The archive folder could have been deleted.	Check whether the archive id folder exists under *NMSROOT/* files\rme\jobs\inventory\reports \archives If the folder does not exist: 1. Delete the archive from the UI 2. Create another job to create an archive.
INVREP0030	Could not get device IDs from DCR.	Check whether the DCR Server is running	If the DCR Server is not running, restart it.
INVREP0031	Job not found.	The job folder or the job object may not exist under *NMSROOT/* files\rme\jobs\inventory \reports\jobs.	If the folder does not exist, delete the job from the Job Browser.
INVREP0032	Graph generation failed.	You may not have enough disk space.	Check the invreports.log for more details.
INVREP0033	Could not generate Report Print format	Unknown error	Check the invreports.log for more details.
INVREP0034	Report Generation failed.	Unknown error.	Check the invreports.log for more details.
INVREP0035	Could not access the archive on disk.	The archive folder may be deleted.	Check whether the archive id folder exists under *NMSROOT/* files\rme\jobs\inventory\reports \archives If the folder does not exist: 1. Delete the archive from the UI 2. Create another job to create an archive.
INVREP0036	Could not retrieve Device Credential data.	Check whether the DCR Server is running.	Check the invreports.log for more details. If the DCR Server is not running, restart it.
INVREP0037	Could not retrieve device type information.	Check whether the DCR Server is running.	Check the invreports.log for more details. If the DCR Server is not running, restart it.

Message ID	Error Message	Probable Cause	Possible Action
INVREP0038	Could not retrieve device serial number information.	Check whether the DCR Server is running.	Check the invreports.log for more details. If the DCR Server is not running, restart it.
INVREP0039	Could not retrieve user defined fields.	Check whether the DCR Server is running.	Check the invreports.log for more details. If the DCR Server is not running, restart it.
INVREP0040	Database related failure.	Check whether the RME database is running.	Check the invreports.log for more details. If the database engine is not running start the engine and try again.
CRIN0001	Not authorized to delete {0} template(s). Contact your system administrator for further help.	You may not have authorization to perform this task.	Contact your system administrator to get permissions.
CRIN0002	Not authorized to modify template {0}. Contact your system administrator for further help.	You may not have authorization to perform this task.	Contact your system administrator to get permissions.
CRIN0003	Template(s) {0} not found. Check the log for more details.	The templates may have been deleted from another browser or by another authorized user at the same time.	You must recreate the required templates.
CRIN0004	One or more of the selected archives are missing. Check the log for more details.	The archives may have been deleted from another browser or by another authorized user at the same time.	You must recreate the jobs and get the required archives.
CRIN0005	Job(s) {0} not found. Check the log for more details.	The jobs may have been deleted from another browser or by another authorized user at the same time.	You must recreate the jobs.
CRIN0006	Could not get templates from {0}. Check the log for more details.	Either: • There is a specific problem with {0} application. Or • The templates were deleted from another browser or by another authorized user.	Review the specific application log and cri.log. If required, recreate the templates.

Message ID	Error Message	Probable Cause	Possible Action
CRIN0007	Could not get archives from {0}. Check the log for more details.	Either: - There is a specific problem with {0} application. Or - The archives were deleted from another browser or by another authorized user.	Review the specific application application log and cri.log. and recreate the jobs.
CRIN0008	Could not delete templates {0}. Check the log for more details.	The templates may have been deleted from another browser or by another authorized user at the same time.	No workaround.
CRIN0009	Could not delete jobs {0}. Check the log for more details.	The jobs may have been deleted from another browser or by another authorized user at the same time.	No workaround.
CRIN0010	Could not delete jobs{0} in running state.	This is the expected behavior.	You can delete the job after it has completed.
CRIN0011	Could not delete jobs{0} in scheduled state	This is the expected behavior.	No workaround.
CRIN0012	Could not delete one or more of selected archives. Check the log for more details.	The cause will be in the Cri.log.	Check the Cri.log for the probable cause and action.
CRIN0013	Could not get template details for {0}. Check the log for more details.	Either: - There is a specific problem with {0} application. Or - The templates were deleted from another browser or by another authorized user.	Review the specific log and cri.log. If required, recreate the templates.
CRIN0014	Operation failed, caused by failure in connecting to JRM. Make sure jrm and/or CTMJrmWrapper services are running.	JRM or CTMJrmServer services may not be running.	Start JRM and CTMJrmServer. To do this use the commands, pdstart jrm and pdstart CTMJrmServer
CRIN0015	Could not apply purge settings. Check the log {0} for more details.	The cause will be in the Cri.log.	Check the Cri.log for the probable cause and action.

Message ID	Error Message	Probable Cause	Possible Action
CRIN0016	Registration with CCR failed or no related entries found in CCR registry. Check cri.log for more details or contact System Administrator for more help.	CCR entry is not done for the required archive setting.	Check cri.log and contact System Administrator for further help.
CRIN0017	Directory {0} not found. Choose valid directory for setting the new archive location.	Chosen directory might not exist.	Create a new directory at required location and choose the same again.
CRIN0018	You do not have write permission to {0}. Select the directory to which you have write permission.	No write permission to the selected folder.	Select the folder one to which you have write permission or change permissions to the current chosen folder.
CRIN0020	Changing reports archive location failed. Check the cri.log for more details.	Some other user may be accessing archives or job is running.	While changing the archive location, make sure that no job is running or no archives are accessed. Otherwise this task will not succeed.
CRIN0021	Moving the report archives to the chosen location failed. Check the cri.log for more details	This may be caused by any of the following: • Some other user may be accessing archives or job is running. • You may not have write permission to that folder. • Disk space may not be sufficient.	• Check the cri.log for more details. • Make sure that no archives are accessed or no job is running while moving archives to new location. • Make sure that the new location has more free space than the old archive directory size.
Not Applicable	Inventory Report job remains in the running state forever.	The default runtime memory is set as follows: Minimum heap size: 128 MB Maximum heap size: 512 MB If the job requires heap size more than 512 MB, then the job will have insufficient memory and will hangs or fail displaying this message: `out of memory`	1. Cancel the currently running job. 2. Increase minimum and maximum heap in the following file: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\inventory\reports\datagenerators\IRConfig.properties to 512 MB and 1024 MB respectively. 3. Schedule another job.

Archive Management

This section provides the troubleshooting information and FAQs for the Archive Management application:

- Archive Management FAQs
- Troubleshooting Archive Management

Archive Management FAQs

- Q.Can I define the protocol order for configuration fetch and deploy?
- Q.I have set up the purge setting for configuration files to retain 3 versions and no version older than 5 days. This purge job runs daily. The configuration files are deleted for the selected versions but the configuration diff files still exist for the deleted versions. Why does this happen?
- Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?
- Q.How Configuration Management interprets device credentials?
- Q.What are the supported device prompts?

Q. Can I define the protocol order for configuration fetch and deploy?

A. Yes, you can define the order of protocol that has to be used for Configuration Management applications (Archive Management, Config Editor, and NetConfig). You can define this in the Transport Settings window (**Resource Manager Essentials > Admin > Config Mgmt**).

Q. I have set up the purge setting for configuration files to retain 3 versions and no version older than 5 days. This purge job runs daily. The configuration files are deleted for the selected versions but the configuration diff files still exist for the deleted versions. Why does this happen?

A. The configuration diff files are not purged because the RME Change Audit records refer to these files. After you delete the RME Change Audit records, these configuration diff files get deleted automatically.

Q. When I select:

a. TFTP alone as the configuration transport protocol

b. Run Sync Archive Job for a device

c. Run a data capture trace

The data capture trace shows Telnet traffic along with SNMP/TFTP sessions.

Why does the Telnet session appear in the data capture trace although I have selected TFTP as the configuration transport protocol?

Q. The Telnet session that appears in the data capture trace is a socket connection to the Telnet port. It identifies the IP address of the CiscoWorks RME server. This is important in multi-homed servers where the IP address that CiscoWorks server uses to contact the device, has to be identified.

Q. How Configuration Management interprets device credentials?

A. You can enter the device credentials when you,

- Add/import devices using Common Services Device and Credential option (**Common Services > Device and Credentials > Device Management**). In this flow, you can enter:

  - Primary Username—User name for the device.
  - Primary Password—Password for the device.
  - Primary Enable Password — Console-enabled password for the device.
- If you have enabled Enable Job Password option (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies)** then while scheduling for a job, you can enter these credentials:
  - Login User name—User name for the device.
  - Login Password—Password for the device.
  - Enable Password—Console-enabled password for the device.

  These credentials are used while running the job. The credentials that you have entered in the Device and Credential Repository are ignored while running the job.

TACACS (Terminal Access Controller Access Control System) uses a separate centralized server to track usernames and passwords. This simplifies authentication and authorization, because information is maintained in only one database rather than being spread out over many devices.

If your devices are configured to use TACACS, you must provide TACACS device credentials when you add or import the devices.

See Q.How are the device credentials mapped in Device and Credential Repository? for information on how Device and Credential Repository maps the device credentials.

Login Authentication in Telnet Mode

When RME logs into non-privileged mode (User mode), depending on your device authentication configuration, the device will prompt for either username and password, or password only.

If the device prompts for username and password, RME responds with the following:

- If Primary Username and Primary Password credentials are entered in the Device and Credential Repository, RME sends Primary Username and Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, RME sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management)** is ignored.
- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password

    Or
  - The Primary credentials or Login User name and Login Password are not present in the database.

  RME reports the login as failure.

If the device prompts for password only, RME responds as follows:

- If Primary Password is entered in the database, RME sends Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, RME sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management)** is ignored.

If you have configured only the Telnet password (without configuring username) on your device. You have to enter some string in the Login Username field. That is, you cannot leave the Login Username field blank.

The Login Username string will be ignored while connecting to the device as the device is configured only for the Telnet password.

- If:
  - Authentication fails with the Primary Password or Login Password

    Or
  - The Primary Password or Login Password is not present in the database.

  RME reports the login as failure.

Login Authentication in SSH Mode

This section describes how the device credentials are interpreted by RME in SSH mode.

Open an SSH session to the device.

The device prompts for username and password, RME responds as the following:

- If Primary Username and Primary Password are entered in the database, RME sends Primary Username and Primary Password to the device.

  If you have enabled Enable Job Password option in the Job Policy dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, RME sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management)** is ignored.
- If:
  - Authentication fails with the Primary credentials or Login User name and Login Password

    Or
  - The Primary credentials or Login User name and Login Password are not present in the database

  RME reports the login as failure.

Enable Login Authentication in Telnet Mode

This section describes how the TACACS and other credentials are interpreted by RME in Telnet mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. RME logs into non-privileged mode (See Login Authentication in Telnet Mode).
2. If logging into non-privileged mode is successful, RME issues "enable" command for the device to enter into privileged mode.

   If the device prompts for password, RME responds as follows:
   - If Primary Enable password is entered in the database, RME sends Enable Primary password to the device.

     If you have enabled Enable Job Password option in the Job Policy dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, RME sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management)** is ignored. .

  - If authentication fails or Enable Password or Primary Enable Password is not present in database

    or

  - If logging into non-privileged mode fails or authentication fails in all above cases.

    RME reports the login as failure.

Enable Login Authentication in SSH Mode

This section describes how the TACACS and other credentials are interpreted by RME in SSH mode.

Logging into the Privileged mode (Enable mode) involves two steps:

1. RME logs into non-privileged mode (See Login Authentication in SSH Mode).
2. If logging into non-privileged mode is successful, RME issues the **enable** command for the device to enter into privileged mode.

   If the device prompts for password, RME responds as follows:

   - If Primary Enable Password is entered in the database, RME sends Primary Enable password to the device.

     If you have enabled Enable Job Password option in the Job Policy dialog box (**Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies**) and if you have entered the Login Password at the time of scheduling a job, RME sends the Login Password entered in this dialog box. The Primary Password entered in the Device and Credential Repository (**Common Services > Device and Credentials > Device Management)** is ignored.

   - If authentication fails or Enable Password or Primary Enable Password is not present in database

     or

   - If logging into non-privileged mode fails or authentication fails in all above cases.

     RME reports the login as failure.

See the Device Management FAQs section to understand the device credentials mapping in Device and Credential Repository.

Q. What are the supported device prompts?

A. The supported device prompts are:

The supported Device authentication prompts are:

- Routers

  “Username:”, “Username: ”

  “Password:”, “Password: ”

- Switches

  “username: ”, “Username: ”

  “password: ”, "Password: ”

- Cisco Interfaces and Modules — Network Analysis Modules

  “login: ”

  “Password: ” “password: ”

- Security and VPN — PIX

“username: ”, “Username: ”

“passwd: ”, “password: ”, “Password: ”

- Content Networking—Content Service Switch

  “Username: ”, “username: ”, “login: ”,“Username:” , “username:” , “login:”

  “Password: ”, “password: ”, “passwd: ”,”Password:” , “password:” , “passwd:”

- Content Networking — Content Engine

  “Username: ” ,”login: ”

  “Password: ”

- Storage Networking — MDS Devices

  “Username:”, “Username: ”

  “Password:”, “Password: ”

Troubleshooting Archive Management

Message ID	Error Message	Probable Cause	Possible Action
CM0003	Version $1 does not exist in archive $2	Version may have been deleted	None
CM0005	Archive does not exist for $1	Error during archive creation.	Check the file system/user privileges.
CM0006	Archives do not exist	Error during archive creation.	Check the file system/user privileges.
CM0008	Checkout not permitted on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0010	Checkin not permitted on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0011	Delete not permitted	You may not have the required permission	Check with the administrator for your privilege.
CM0012	Could not create new version on archive $1	Insufficient disk space or config file may be incomplete.	Check whether disk space is available and that the directory has required permissions
CM0013	Cannot delete version on archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0015	Could not check out config for archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0016	Could not undo check out config for archive $1	You may not have the required permission	Check with the administrator for your privilege.
CM0017	Could not check in config for archive $1	$2	Check whether the file system is full and if you have required permissions.
CM0021	Version does not exist in archive $1	Version may have been deleted	None
CM0022	Archive already exists	Archive names should be unique	Enter a different name
CM0023	Archive creation not permitted	You may not have the required permission	Check with the administrator for your privilege.

Message ID	Error Message	Probable Cause	Possible Action
CM0024	Error while deleting archive	You may not have the required permission	Check with the administrator for your privilege.
CM0025	Cannot delete device archive	Only the system purge can delete the device archive	Schedule for a purge job.
CM0026	Archive Relocation failed	The destination folder may not have the required disk space or required permission.	• Check if the destination folder has the required permission • Check if the disk space is available • Check if the user has the write permission.
CM0034	Cannot list versions for $1	You may not have the required permission or version do not exist.	Check with the administrator for your privilege.
CM0037	Database Connection Error	Database Engine may be down	Restart the RMEDbMonitor and CmfDbMonitor services
CM0038	Error in Database	Database Engine may be down	Restart the RMEDbMonitor and CmfDbMonitor services
CM0040	Error while reading the file from the system	Either: • The file may not exist Or • You may not have required permissions.	Verify whether you have the correct privileges and that the file system is not corrupted.
CM0041	Error while writing the file to the system	Either: • The file may not exist Or • You may not have required permissions.	Verify whether you have the correct privileges and that the file system is not full
CM0043	Error while copying the file	Either: • The source or destination file may not exist Or • You may not have required permissions.	Verify whether: • The files exist • The file system is not full. • You have permission
CM0050	Cannot compare the configurations since they are not of the same type.	Configuration types are different	Select device of the same type.
CM0051	Cannot connect to ConfigMgmtSever process	Process may be down or maximum connection have been reached.	Restart the ConfigMgmtSever process.

Message ID	Error Message	Probable Cause	Possible Action
CM0054	Error while initializing Transport for $1	Device packages may not exist.	Check whether: • The user exists in RME and has required permissions, • Device is reachable • Required device packages are available in RME.
CM0076	Job creation failed	$1	Check whether Jrm and CTMJrmServer processes are running
CM0077	Job modification failed	$1	Check whether Jrm and CTMJrmServer processes are running
CM0080	Could not send e-mail.	The e-mail configuration in your profile may be either missing or incorrect	Check e-mail configuration.
CM0082	Job execution failed.	The job policy may not be enabled	Enable the policy and try again
CM0085	Cannot list jobs of type	Jobs of this type may not exist in RME.	Enable the policy and try again.
CM0086	Cannot load job with id.	Job may not exist in RME	Verify that the Job ID exists and try again
CM0087	Cannot obtain lock on device	Another application/job may have locked the device.	Verify that there are no other jobs is running on the device. Retry the job after some time.
CM0088	Configuration archival failed for $1	Not enough disk space.	Check whether the device is reachable and that the credentials are correct.
CM0090	Reload task failed on device	Device many not be reachable.	Check whether the device is reachable and that the credentials are correct.
CM0096	Job ID is not valid	The job may not exist in RME	Verify that the job exists and try again.
CM0097	No failed devices in the job	There may not be any failed devices in the job.	Check for failed devices and try again.
CM0098	Invalid Job-based password specified	The Job-based password data may be null or cannot be used.	Enter the correct Job-based password and try again.
CM0109	Cannot read admin preferences.	Application may not have been initialized correctly	Retry the task
CM0122	No commands to write.	Command may not be available	Verify whether there are any commands to deploy
CM0123	Exception while getting all baseline templates.	Templates may have been deleted	Check if the template exist.
CM0125	Cannot persist template.	Template may be empty or invalid.	Check whether the commands are valid
CM0126	Cannot find baseline archive $1	Archive may have been deleted	Check if the archive exist.
CM0128	Cannot get baseline branch.	Branch may not exist.	Check if the branch exist.
CM0131	Cannot find template	Template may have been deleted	Check if the template exist.

Message ID	Error Message	Probable Cause	Possible Action
CM0132	Cannot find result for job	Job may not exist.	Check if the job has been deleted.
CM0133	Invalid check-type for command	Check type may be invalid	Verify if the check-type is valid.
CM0136	Regular expression match failed.	Not a valid Regular expression.	Check if the expression is valid.
CM0137	No commandlets.	None	None
CM0138	Cannot find result for device	Device has been deleted.	Check if the device exist.
CM0139	Could not archive configuration	File system may be full or user may not have the required permission.	Check whether device is reachable and device credentials are correct. Increase timeout value, if required.
CM0148	User or device authorization failed.	User may not exist or does not have privileges to operate on any or all of the devices in the job.	Check whether the user exists and has required privileges to execute jobs.
CM0201	Could not start the SdiEngine.	The package path may be incorrect	Check whether the specified package path is correct
CM0202	Could not access the device using SNMP.	SNMP may be disabled on the device,	Check the Read Community string
CM0203	Could not create the CIDS Device Representation for device	Device package may not exist	Check if the required device packages are installed.
CM0204	Could not create Device Context for the device	Device package may not exist	Check whether the required device packages are available in RME.
CM0205	Device package not found	Device package may not exist	Check whether the required device packages are available in RME.
CM0206	Could not get the configuration transport implementation for $1	Device package may not exist	Check whether the required device packages are available in RME.
CM0207	Could not get configuration analyzer implementation for $1	Device package may not exist	Check whether the required device packages are available in RME.
CM0210	Cannot generate processed configuration	Configuration file may be corrupted or incomplete	Check that device returns complete configuration and the configuration file is not empty.

NetConfig

This section provides the troubleshooting information and FAQs for the NetConfig application:

- NetConfig FAQs
- Troubleshooting NetConfig

NetConfig FAQs

Q.What are the supported protocols for NetConfig Reload task?

Q. What are the supported protocols for NetConfig Reload task?

A. The supported protocols for NetConfig Reload task are Telnet, SSH and TFTP.

SSH and TFTP protocols are supported by NetConfig Reload task only if these protocols are also supported by the devices.

Troubleshooting NetConfig

This section provides the troubleshooting information for the NetConfig application:

Message ID	Error Message	Probable Cause	Possible Action
CFG0025	Cannot retry.	Retry is not supported on periodic jobs.	None.
CFG0026	You can retry only failed jobs.	A Successful job has been selected instead of a Failed job.	Select a Failed job and try again.
CFG0029	Job approval is enabled.	You have scheduled a job that requires Job approval with the Immediate schedule type. The job will run only when it has been approved by the Approver.	Do not select Immediate job type while scheduling the job.
CFG0009	Error occured while processing.	Check netconfigclient.log for more details.	Retry the operation. If the problem persists, send the logs to Cisco Technical Assistance Center (TAC). The netconfig logs are available at this location: On Windows: *NMSROOT*`\log\netconfigclient.log` On Solaris: `/var/adm/CSCOpx/log/netconfigclient.log`
CFG0029	Job approval is enabled.	This job requires job approval. So it can run only when the job is approved. So you cannot schedule a job with immediate schedule type.	Do not select Immediate schedule type.
CFG0041	You have selected an instance that does not have a task associated with it.	None.	Select an instance that has an associated task.

Config Editor

This section provides the troubleshooting information for the Config Editor application:

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0001	No device selected	You have not selected a device.	Select a device and try again.
CEDT0002	There is no configuration file for the device.	There is no configuration file for the selected device in the archive.	Perform Synch Archive to get the configuration file for the device
CEDT0003	Modified Config not selected.	You have not selected a modified configuration from the Modified Configs list.	Select a configuration file from Modified Configs list.
CEDT0004	No Config Selected for Download.	You have not selected a configuration file for downloading either from the archive or from Modified Configs list.	Select a configuration file for downloading either from the archive or the Modified Configs list.
CEDT0005	Enter job description.	You have not entered a job description while creating a job	Enter the job description. This is mandatory.
CEDT0007	No job selected.	You have not selected a job.	Select a job
CEDT0009	Job {JobId} cannot be {Action}.	You have tried to do any of the following: • Edit a completed job • Copy an incomplete job • Stop a completed job • Stop an already stopped job.	Select the appropriate job and appropriate action.
CEDT0010	Cannot get details for Job {JobID}.	The Job was recorded incorrectly.	None.
CEDT0011	Could not get the summary of the job.	None.	Check Cfgedit.log for more details.
CEDT0012	Job not found.	None	Check Cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.
CEDT0013	Some change in Jsp leading to incompatible with Action class.	None.	Check cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.
CEDT0014	Label not selected for search	You have tried to search labeled configurations without selecting a label	Select a label from the drop down.
CEDT0015	Cannot open configuration file.	None.	Check Cfgedit.log for more details. Contact Cisco TAC with log details for further assistance.

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0016	Cannot open Baseline Template.	Template may be deleted	Check whether the template exists.
CEDT0017	Baseline Templates not present for the selected device.	There are no templates for the selected device type.	Create a Baseline Template for the selected device type from the archive.
CEDT0018	No Config found for the specified search pattern	The pattern you have entered cannot be found in any of the configs	Change the search pattern.
CEDT0019	External Config to be opened not selected	You have not selected an External Config.	Select the External Config File from the browser.
CEDT0020	Invalid configuration file.	Configuration file is corrupted.	Recreate config.
CEDT0021	Version to be opened not selected.	None.	Select a valid version
CEDT0022	Cannot load query. Check whether the query exists.	The query you selected may have been deleted.	Use Config Mgmt > Archive Mgmt> Search Archive> Custom Queries to check whether the query exists. Create a query if it does not exist.
CEDT0023	Cannot find query. Check whether the query exists	The query you selected may have been deleted.	Use Config Mgmt > Archive Mgmt> Search Archive> Custom Queries to check whether the query exists. Create a query if it does not exist.
CEDT0024	No External Syntax Checker is registered with CMIC.	Either: • You may have launched the External Syntax checker without registering the syntax checker tool with CMIC. or • The syntax checker is not registered correctly with CMIC.	Register the syntax checker tool correctly with CMIC before Launching External Syntax checker.
CEDT0025	Syntax Checking functionality is not supported by this device image.	The device image you have selected does not support Syntax Checking functionality.	Select another device image that supports Syntax Checking functionality.
CEDT0029	One or more of the devices selected are already added to this job.	A config for the device has already been added	Only one config can be downloaded to a device in a Job.
CEDT0030	No configuration file exists for the device	There is no configuration file for the selected device in the archive.	Perform Synch Archive to get the configuration file for the device
CEDT0031	There are no commands to download.	None.	Remove the device from job and try again.

Message-ID	Error Message	Probable Cause	Possible Action
CEDT0032	Approval is enabled. Cannot schedule immediate jobs.	You cannot schedule Immediate jobs if Approval is enabled.	Select Schedule type, Once instead of Immediate
CEDT0033	Selected Job Execution date is invalid.	You have selected a past date for running a job.	Select a valid future date.
CEDIT0034	Job user name or password not entered.	You have enabled the Job based password option but not entered password.	Either: • Deselect the Job-based password option Or • Enter the user name and password fields.
CEDT0039	Enter at least one pattern.	You have not entered any search patterns.	Either: • Select one of the queries listed Or • Enter a search pattern.

Software Management

This section provides the troubleshooting information and FAQs for the Software Management applications:

- Software Management FAQs
- Troubleshooting Software Management

Software Management FAQs

- Q.What are the high-level features of Software Management 4.1?
- Q.What privilege level is required to run Software Management functions?
- Q.How do I know which functions I can access in Software Management?
- Q.Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?
- Q.Can I use Remote Copy Protocol (RCP) to transfer images to devices?
- Q.What connection mechanism does Software Management use to upgrade software?
- Q.What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?
- Q.Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?
- Q.Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?
- Q.What is Job Approval?
- Q.What is the approver list?
- Q.Is the Job Approval policy enforced system-wide?
- Q.How do I configure Job Approval for Software Management?
- Q.Which Cisco IOS devices support bootldr images?

- Q.How do you identify bootldr image files?
- Q.How does the Software Management bootldr recommendation process work?
- Q.Where is the storage location of the bootldr image on the Cisco IOS device?
- Q.Does Software Management erase bootflash if there is not enough free space on bootflash?
- Q.Does Software Management change the configuration file for bootldr upgrades?
- Q.Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?
- Q.Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?
- Q.Can I upgrade modules on the device using advanced Distribution mode?
- Q.What image extension type are not supported in Software Management?
- Q.How can secured image upgrades be performed using Software Management?
- Q.How to use Reboot order configuration feature?
- Q.Is Image import from URL is treated as separate Job?
- Q.What is the best effort verification performed while distributing the image using Advance mode?
- Q.When does Software Management Application use SSH?
- Q.How can a protocol be Enabled/Disabled for a job?
- Q.How are devices upgraded using Secured Copy Protocol?
- Q.How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?
- Q.What is the swap file size required for Software Management application?
- Q.What Version of SCP is supported in Software Management application?
- Q.What are the pre requisites for using SCP for image upgrade?
- Q.Why is the job still running after I cancel it?
- Q.Why do I get an error message such as, `Navigation to other areas of this application is not available until the opened wizard is finished or canceled.`?
- Q.The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?
- Q.I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?
- Q.During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking Next. However, the results may be inaccurate.”?
- Q.Why am I not able to see the Immediate option during software management jobs?
- A.Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.
- Q.I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.
- Q.I am not able to select a user script which is in xxx path.

- Q.In ACS login mode, I am not able to see links that I usually get to see.
- Q.In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.
- Q.What validations are performed by Software Management before actual image distribution onto the device?
- Q.What is the minimum software version required to be running on the device for Software Management to upgrade the software?
- Q.Can I have a different script for each device in a job?
- Q.What device types can be used as remote stage device?
- Q.What device types cannot be upgraded using remote stage flow?
- Q.What are the pre-requisites for using the device as remote stage?
- Q.What Configuration changes are performed by Software Management on the remote stage device?
- Q.If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?
- Q.Are there any Bad version of IOS for Remote stage device?
- Q.Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?
- Q.How many devices in a job can be upgraded using remote stage?
- Q.Can I perform Parallel upgrade using remote stage flow?
- Q.Can I perform Slam dunk upgrade using the remote stage?
- Q.What is the difference between Run-from-RAM and Run-from-Flash devices?
- Q.When does Software Management use the remote copy protocol (rcp) to transfer images?
- Q.How does Software Management ensure that file corruption does not occur during transfer?
- Q.After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?
- Q.How much temporary space do you need during image distribution?
- Q.Is Cisco.com connection mandatory for Software Management?
- A.Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.
- Q.How does Software Management handle proxy environments?
- Q.Does Software Management support proxy with user authentication environments?
- Q.Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?
- Q.How come the Cisco.com filter option does not work in LS1010 devices?
- Q.Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?
- Q.Why I cannot download crypto images?
- Q.How does Software Management verify the integrity of the images after importing them from Cisco.com?
- Q.Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?

- Q.What is a Dual Flash Bank device?
- Q.Does Software Management support software upgrades on dual RSP-based systems?
- Q.Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?
- Q.Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?
- Q.How do you change the IP default gateway configuration to allow Software Management to upgrade a device?
- Q.Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?
- Q.How is the job directory organized?
- Q.Which modem cards does Software Management support?
- Q.Which devices and software versions get support for the modem upgrades?
- Q.Which formats of Microcom firmware images does Software Management support?
- Q.Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?
- Q.Why does the Undo option not receive support for modem upgrades?
- Q.What connection mechanism does Software Management use for modem upgrades?
- Q.Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?
- Q.What is CIP?
- Q.Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?
- Q.What is the minimum Channel Interface Processor (CIP) version that Software Management supports?
- Q.How can you import Channel Interface Processor (CIP) images to the Software Management library?
- Q.Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?
- Q.What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?
- Q.Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?
- Q.Does Software Management supports CIP2?
- Q.In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?
- Q.Does the Supervisor Engine card reboot after the upgrade of all modules?
- Q.Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?
- Q.Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?

- Q.Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?
- Q.Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?
- Q.Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?
- Q.Do you need to reconfigure the device when you downgrade the Supervisor Engine software?
- Q.In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?
- Q.Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?
- Q.Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?
- Q.How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?
- Q.How can I make the Image Recommendation faster?
- Q.Why do the software version numbers that the show module command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?
- Q.Does Software Management recommend the right ATM image for your ATM module type?
- Q.Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?
- Q.How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?
- Q.Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?
- Q.How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?
- Q.Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?
- Q.What is the minimum version that Cisco 700 series ISDN routers support?
- Q.What connection mechanism does Software Management use for Cisco 700 series upgrades?
- Q.Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?
- Q.Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?
- Q.Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?
- Q.Why does Software Management report download failures for some images even though the device runs the new image after the job completes?
- Q.In which order does Software Management upgrade modules on a Catalyst 5000 device?
- Q.Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?

- Q.Does Software Management support upgrading software on redundant Supervisor card-based systems?
- Q.What is the purpose of user scripts?
- Q.What if the user script crashes? Will it crash the Software Management job also?
- Q.When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
- Q.Can I set up a periodic download of Software Management images from Cisco.com?
- Q.Is browser timeout something I should consider when downloading?
- Q.What are crypto images?
- Q.How much temporary space is required during image distribution?
- Q.At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
- Q.How can I speed up Image Recommendation?
- Q.When a job is rejected, can it be edited or should I resubmit?
- Q.Can different group members edit jobs? What are the restrictions?
- Q.What is the role of the registry files in RME?
- Q.How do I upgrade Network Analysis Module (NAM) using Software Management?
- Q.Can I change the job scheduled time?
- Q.How does Software Management handle the job status for an abnormally terminated job?
- Q.How does Software Management handle the job status of a pending job whose scheduled time has passed?
- Q.Why are some files left in the Software Management folder after Software Management has been uninstalled?
- Q.How can I enable or disable the SSH to Telnet fallback for RME - Software Management jobs?
- Q.How can I export the images from RME-SWIM repository to a local drive or a file system mounted to the RME server?
- Q.Does flash get erased if there is no sufficient space for Patch Distribution?
- Q.When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.
- Q.No information is logged in the log file for Software (SWIM) CLI.
- Q.Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI `exportimages` command?

Q. What are the high-level features of Software Management 4.1?

A. Software Management offers the following management functions:

- Software Distribution — Schedules download of software images to a single device or groups of devices. Hardware and firmware validation verifies whether the new image can run on the device. Image Upgrade can be performed in Sequential or in parallel. Also the In Parallel mode of upgrade device reboot can be controlled for the job.

  Provides several workflow to achieve this functionality

  - Distribute By Device [Basic]

  - Distribute [Advance]
  - Distribute by Image
  - Distribute by Remote Stage/ External TFTP server
  - Patch Distribution
- Software Repository — Builds and maintains a library archive of software images. Software images can be added to repository from,
  - Device— Allows to archive the current software images on the device
  - Cisco.com— Integrates with Cisco Connection Online (Cisco.com) to download software images.
  - File System—Allows to import an image from a directory accessible from the RME server
  - Network—Allows the library to synchronize with the software images running on the devices. A periodic job can generate a list of images that are not in the library. You then have the option to import new images into the library and check them for discrepancies between software images running on the network and images in the library.
  - URL—Allows to download images from URL you specify.
- Upgrade Analysis—Determines the hardware upgrades required on network devices to enable them to run new software. Software Management allows analysis based on the location of image to be analyzed. Following locations are supported.
  - Cisco.com
  - Local Repository
- Job Management
  - Job Approval — Allows organizations to require approvals before allowing software upgrades.
  - Software Management jobs can be operated upon to,

    Retry

    Undo

    Cancel

    Stop
- Reports
  - Work order — Displays changes that will be made to network devices as part of the software upgrade.
  - Synchronization report — Displays which Software Management-supported devices are running software images that are not in the software image repository.
  - Audit trail—Tracks software changes made on the RME server

Q. What privilege level is required to run Software Management functions?

A. Different options in Software Management require different levels of user privileges. Privilege levels are known as “roles” in RME. For a list of RME functions and required user roles, use the Permissions Report function (**Common Services > Server > Reports**).

Q. How do I know which functions I can access in Software Management?

A. To find which functions you can access in Software Management:

- Select **Common services > Server > Reports > Who Is Logged On** to find your assigned roles.

- Select **Common services > Server Reports > Permissions Report** to verify which RME and Software Management tasks you can run.

Q. Are there DNS dependencies for Remote Copy Protocol (RCP) to work properly for a device?

A. Yes. If there are multiple IP addresses configured on the device, all IP addresses on the device must be configured in the Domain Name System (DNS). Examples of devices with multiple IP addresses are those having many interfaces, with each interface configured with its own IP address, or a device that interfaces configured with primary and secondary IP addresses.

Configure the DNS so that all IP addresses are resolved to the same host name. The host name in the DNS should match the host name entered in the Device and Credential Repository.

Q. Can I use Remote Copy Protocol (RCP) to transfer images to devices?

A. Use the RCP transport protocol for image transfers only on Cisco IOS devices that support the CISCO-FLASH-MIB. Catalyst switches that run Supervisor software older than 5.2, and 700 Series devices do not support the RCP protocol.

The Cisco IOS devices can not use RCP if they only support OLD-CISCO-FLASH-MIB, (for example, MC3810) or if they do not support any Flash Management Information Base (MIB) (for example, RSP 7000 devices running Cisco IOS Software Releases 10.3-11.0).

Q. What connection mechanism does Software Management use to upgrade software?

A. Simple Network Management Protocol (SNMP) is the preferred mechanism used by Software Management to upgrade software. Some devices, however, cannot be upgraded using SNMP alone.

For such devices, Software Management uses a Telnet interface to do the upgrades. SNMP upgrades all Run-from-RAM Cisco IOS devices, Dual Flash Bank Run-from-Flash (DFB RFF) devices, and all Catalyst switches. If SSH is preferred for device connection then SSH is Used for connecting to the device.

Software Management uses Telnet to perform the following upgrades:

- Single Flash Bank Run-from-Flash Cisco IOS devices (SFB 2500s, 1600s, AS5200)
- RSP 7000 devices running Cisco IOS Software Releases 10.3 - 11.0
- Cisco 700 Series
- CIP, MICA, Microcom upgrades
- 3500/2900 series of devices
- 1900/2820 Series
- VPN 3000 Series of devices.

For complete list of supported protocols see Supported Device Table for Software Management.

Q. What is the default Simple Network Management Protocol (SNMP) timeout used by Software Management? Can I configure it?

A. Default retry is 2 and default SNMP time out value is 2. This value is configurable using **RME > Admin > System Preference**.

Q. Can I configure TACACS or Radius authentication for devices that Software Management has upgraded?

A. Software Management supports upgrading devices that are configured for TACACS or Radius authentication. An exception is software upgrades on the Run-from-Flash partition if the device is configured with Radius protocol authentication. The Common Services Device and Credential Repository must be configured with the appropriate information to access the device.

Q. Can I configure default privileges on terminal lines for Cisco IOS devices that Software Management has upgraded?

A. Software Management upgrades software by using the Telnet interface or Command-Line Interface (CLI) on devices that do not support enough Management Information Base (MIB) instrumentation for software management.

Software Management uses Telnet to connect into the devices and executes privileged commands such as copy tftp flash, copy flash tftp, erase flash, show version, copy flash modem to perform upgrades.

Software Management modifies the configuration file using the Telnet interface to upgrade the software. For Software Management to work on a device, there are some restrictions on how default privileges and enable mode authentication are configured.

The restrictions apply to only those Cisco IOS devices that are managed by Software Management through the Telnet interface. Cisco 700 Series and Catalyst 5000/6000/4000 devices are not affected. Restrictions include the following:

- Software Management tries to run the above CLI commands from privilege level 15. The user must always configure an enable password/secret for privilege level 15, and the same password/secret must be entered in the Device and Credential Repository.

  If the device is configured with TACACS authentication for enable mode access, then the Enable TACACS user name and password must be entered in the Device and Credential Repository. The Enable User name and password authenticated by TACACS+ server always should receive a privilege level of 15.
- The default privilege level configured on a vty line must allow Software Management to run the CLI commands mentioned earlier as well change the configuration file on the device. The privilege level does not need to be 15, but setting the privilege level to 15 guarantees Software Management can always work on the device.

See Q.How are the device credentials mapped in Device and Credential Repository? for information on how Device and Credential Repository maps the device credentials.

Q. What is Job Approval?

A. Job Approval allows an organization to require approvals before an administrator distributes software images. When an image distribution job is created, the administrator (or whoever creates the job) selects from a list of users who can approve the job.

For the job to run, one of the users on the approver list must approve it before its scheduled time. If the job is not approved, it will be rejected at the scheduled time.

Q. What is the approver list?

A. An approver list consists of user names in RME who have the authority to approve software upgrades.

The following steps are required:

a. Create a approver (**Common Service > Server > Security > Single-Server Management > Local User Setup > Add**).

b. Create the list by using the Create Approver List (**Resource Manager Essentials > Admin > Approval > Create/Edit Approver Lists**). Only users who have an Approver role can be added to the Approver List.

Q. Is the Job Approval policy enforced system-wide?

A. Yes. To create a job that does not require approval, disable the Software Management option (**RME > Admin > Approval > Approval Policies)**

Q. How do I configure Job Approval for Software Management?

A. To configure Job Approval, do the following:

a. Add the approver user (**Common Service > Server > Security > Single-Server Management > Local User Setup > Add**).

b. Create an Approver List (**Resource Manager Essentials > Admin > Approval > Create/Edit Approver Lists**)

c. Enable the Job Approval option (**RME > Admin > Approval > Approval Policies > Software Management**)

Q. Which Cisco IOS devices support bootldr images?

A. The following Cisco IOS device families support bootldr images:

- Cisco 4500 and 4700
- Cisco 7500, Route Switch Processor (RSP)-based 7000
- Cisco 7200
- Cisco AS5200, AS5300, and AS5800 Access Servers
- Route Switch Module (RSM) on Cisco Catalyst 5500/5000
- ESR 10K, 10K2 devices

See the Supported Device Table for Software Management application on Cisco.com for further information.

Q. How do you identify bootldr image files?

A. Bootldr image files follow this name convention, *platform-boot-mz.version*

An example is rsp-boot-mz.11.0(17)BT. If the second part (feature part) of the image file name contains “boot”, then the image is a bootldr image. The software library recognizes the file name and imports the image as a bootldr image. Bootldr images earlier than Cisco IOS Software Release 10.3 contain xboot in the feature part of the image. Software Management does not support such images.

Q. How does the Software Management bootldr recommendation process work?

A. Different hardware platforms in Cisco IOS Software have different bootldr images. For example, the bootldr image for the Cisco 4500 device is c4500-boot-mz; the bootldr image for the Cisco 7200 is c7200-boot-mz.

From the library, Software Management determines which bootldr images belong to the same family as the target device. Software Management then recommends the most current of all available images.

Unlike system software images, bootldr images do not have RAM requirements. Therefore, Software Management does not perform prerequisite matches between the device and the image.

Q. Where is the storage location of the bootldr image on the Cisco IOS device?

A. Software Management always uses the bootflash card as the target Flash for the bootldr image. Software Management stores bootldr images on the bootflash card only, even though Cisco IOS Software allows the store of bootldr images on a Flash card.

If you use other Flash cards for the store of bootldr images, problems can occur when you have stored other types of images, such as system software, Microcom, or Modem ISDN channel aggregation (MICA), in the same location.

Q. Does Software Management erase bootflash if there is not enough free space on bootflash?

A. If the bootflash card does not have enough free space to store the new bootldr image, Software Management erases the bootflash to make room for the new boot image. A verification warning alerts you of the bootflash erase.

To see this warning, click the Failure/Warning link in the Status column of the Verify Image Upgrade window.

Software Management backs up and restores files on bootflash with sizes of less than 1 MB.

Q. Does Software Management change the configuration file for bootldr upgrades?

A. Upon bootldr upgrade, Software Management changes the device configuration file such that the configuration file that downloads to the device contains:

Assume that the file name of the newly downloaded bootldr image is c4500-boot-mz.112-13.bin.

- no boot bootldr
- boot bootldr c4500-boot-mz.112-13.bin

Q. Can Software Management back up the current bootldr image while Software Management runs the Distribute Images job?

A. Software Management backs up the system software image only during the Cisco IOS Distribute Images job execution. The backup of bootldr images cannot take place. Use the add images function to import the bootldr image from device to library. (Select **Resource Manager Essentials > Software Mgmt > Software Repository > Add**).

Q. Does Software Management recommend bootldr images from Cisco.com in the Distribute Images function?

A. Yes, Software Management does recommend the download of bootldr images directly from http://www.cisco.com during the Distribute Images job creation.

Q. Can I upgrade modules on the device using advanced Distribution mode?

A. No. Expert flow is not officially tested with all the possible module upgrade scenarios. Current implementation claims only system software upgrades using the expert flow.

Q. What image extension type are not supported in Software Management?

A. The following file/image types are not supported:

```
doc, txt, pdf, xls, ppt, jpg, jpeg, bmp, csv, mpg, au, xml, html, htm, java, class,
tex, ps, pps.
```

Q. How can secured image upgrades be performed using Software Management?

A. Current Version (4.1) supports new protocols such as, SCP and SSH. You can choose the appropriate protocols based on the device support.

For the devices that are upgraded using Telnet/SSH, new feature called Job based password can be enabled for scheduled job. You can specify a temporary password for the upgrade job and it will take precedence over all the credentials in the Device and Credential Repository.

Q. How to use Reboot order configuration feature?

A. This feature is applicable only in case of "parallel" mode of image upgrade. This feature can be used to perform sequential rebooting of devices. You can make this decision based on the network topology or any other deployment policy. The devices will be rebooted in the order specified by you.

Q. Is Image import from URL is treated as separate Job?

A. Yes, the workflow results in a job.

Q. What is the best effort verification performed while distributing the image using Advance mode?

A. Verification in Advance distribution mode is referred as the best effort verification because you can proceed to schedule the image upgrade even without RME inventory data. This is designed to support devices that are not yet managed in CiscoWorks (pre-deployed devices).

Q. When does Software Management Application use SSH?

A. If the device type selected is to be upgraded using the CLI then Software Management application uses SSH (if opted in the preference). Even for fetching information required during the job creation stage, SSH is used.

Q. How can a protocol be Enabled/Disabled for a job?

A. Using the User Interface, **Resource Manager Essential > Admin > Software Mgmt > View/Edit preference**. Available protocols list the Software Management supported protocols. You have to add or remove the protocols to selected protocol order in order to enable or disable the protocol used for image transfer.

Q. How are devices upgraded using Secured Copy Protocol?

A. Image staging and other checks performed before the image distribution remains same for upgrade using SCP. The options such as Flash erasure, Delete, etc. are performed using Cisco Flash mib or old Cisco flash mib only.

The difference lies in the model used for image upgrade.RME positions itself as a client for the Secured Copy options. Devices with SCP server are (like 2650XM) requested to initiate a file transfer job. The image is transferred from RME to the devices.

Q. How much Disk space should be available while performing parallel image upgrade to large number of devices (more than 100)?

A. The amount of disk depends upon the number of images staged in the upgrade job. If the image selected is common for all the devices then disk space required is equal to size of the image. If different images are selected for each job then disk space required is the sum of all the images.

Q. What is the swap file size required for Software Management application?

A. RME 4.0 recommend a swap size of 2MB for managing 300 devices.

Q. What Version of SCP is supported in Software Management application?

A. Current implementation of SCP is based on the fcpsvc library that uses the SSHv1 stack. Current version of SCP supported is 1.0

Q. What are the pre requisites for using SCP for image upgrade?

A. The prerequisites are:

- The device should have an SCP server. Any image having 3DES feature has SCP server in it.
- SSH should be enabled on the device.

Q. Why is the job still running after I cancel it?

A. In Sequential mode, the job stops only after the image upgrade for the current device or module is finished. Canceling a running job does not cancel the software upgrade being performed at that time. The job stops only after the current upgrade is complete.

During this time, the Browse Job Status screen shows that the job is still running. In case of parallel upgrades, when a job is cancelled, the current set of devices being processed will be continued and not stopped. However, new devices will be processed only after the current devices have completed runing.

Q. Why do I get an error message such as, `Navigation to other areas of this application is not available until the opened wizard is finished or canceled.`?

A. Yes, you get this when you are in a wizard (you will see 'Back', 'Next', 'Finish' & 'Cancel' when you are in a wizard at the bottom) and you click any of the other navigational links.

Q. The Cisco.com profile window is sometimes filled with user and password and sometimes not. Why?

A. If the Cisco.com user name and password is configured for you the same will be pre-populated. You can configure the Cisco.com credentials in the Cisco.com User Account Setup dialog box (**Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup**).

Q. I am not able to select both sequential execution and sequential reboot at 'Schedule Job' step during distribution?

A. If you had selected execution to be sequential the same order applies to reboot. However, if the execution is parallel you will be allowed to select reboot sequential.

Q. During Distribution by Advance flow, I get “Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify once again. If you do not edit the expert input file, you can continue with the task by clicking **Next**. However, the results may be inaccurate.”?

A. You get this when there are no inventory information available for the device. You can expect this error for 2900, 3500, 3550 xl devices.

Q. Why am I not able to see the Immediate option during software management jobs?

A. Check if approval is enabled. If approval is enabled for Software Mgmt Jobs, you will not be able to schedule Immediate job.

Q. I am not able to select the device (greyed box) at Software Management device selector page, but I'm able to select at inventory.

A. Software Management support might not be there. See the Supported Device Table for RME 4.1 on Cisco.com

Q. I am not able to select a user script which is in xxx path.

A. The scripts are expected to be available in the specific path. *NMSROOT*/files/scripts/swim is the location for Software Management scripts.

Where *NMSROOT* is the CiscoWorks installed directory.

Q. In ACS login mode, I am not able to see links that I usually get to see.

A. On the ACS server, check if some role to task mapping (tree) has got changed. The required Software Management task option should be selected on the ACS server for a particular role.

Q. In the Job Details Window (clicking on job ID in the Software Management Job Browser) I don't see the job status being updated.

A. The job status will not be updated, as only the job running status is getting refreshed.

Q. What validations are performed by Software Management before actual image distribution onto the device?

A. Software performs the following checks before the job execution:

- Checks whether job file is Available at the job id and has required data in the format and prepares a list of devices to be upgraded in the job.
- Checks whether RME License is valid
  - Whether license file is valid
  - Number of devices managed
- Removes all devices from the list which are not authorized for the user to perform image distribution.

  Removes all devices from the list which are in Suspended state or Conflicting state. Pre-deployed state devices are not removed.
- Checks for the proper pre/post job script (if any) ownership and permission
  - On Solaris, check is performed for `rwxr-x---` permissions for script file (0750)
  - On Windows, check is performed if the given script has write permissions for any non-admin and non-casuser
- Verifies that critical data required for image upgrade are present in the job file.

Q. What is the minimum software version required to be running on the device for Software Management to upgrade the software?

A. For Cisco IOS device minimum supported version is 11.0 where as for Catalyst Images Minimum supported version is 3.8.

For more details on minimum supported version for each device type see the Supported Devices Table for Resource Manager Essentials 4.1

Q. Can I have a different script for each device in a job?

A. No, you cannot have separate script for each device.In Software Management 4.1, script is defined in admin preference option and is common for all Software Management jobs.

Q. What device types can be used as remote stage device?

A. All IOS devices with running image version >=12.0 version and complete CISCO-FLASH-MIB support can be used as Remote-Stage device.

Q. What device types cannot be upgraded using remote stage flow?

A. Content Engines (CE), Network Analysis Modules (NAM), Content Service Switches (CSS), and PIX.

Q. What are the pre-requisites for using the device as remote stage?

A. It must be an IOS device and it must be running >= 12.0 version and it must support CISCO-FLASH-MIB completely.

Q. What Configuration changes are performed by Software Management on the remote stage device?

A. tftp-server *flash-partiiton-name:image-nam*e alias *image-name* is the only command that will be added to the Remote stage device to make the image copied to Remote Stage device as accessible through TFTP from other devices.

Q. If I use the device as remote stage device does it impact the device's other functionalities? or what are the performance implications of using the device as remote stage device?

A. There will not be any impact on device's other functionalities and also they will no be any performance implications on the device that is used as Remote-Stage.

Q. Are there any Bad version of IOS for Remote stage device?

A. 12.3(5x) series.

Q. Can I perform module upgrade (like Bootloader/mica/microcom etc.) using remote stage flow?

A. No.

Q. How many devices in a job can be upgraded using remote stage?

A. There is no limit specific to remote stage flow.the number of devices in a remote stage job is same as that of other distribution flow.

Q. Can I perform Parallel upgrade using remote stage flow?

A. Yes

Q. Can I perform Slam dunk upgrade using the remote stage?

A. No. The image that you want to use must be in the Software Repository.

Q. What is the difference between Run-from-RAM and Run-from-Flash devices?

A. Most Cisco IOS devices load the software image from Flash to RAM when rebooting, then run the software from RAM. Such devices are called Run-from-RAM (RFR) devices. For these devices, the software image on Flash can be upgraded without rebooting the device.

Certain Cisco IOS devices (namely 2500s, 1600s, and AS5200s) run the system software image directly from Flash. These are Run-from-Flash (RFF) devices. The Flash partition in which the current image is stored is the RFF partition, which is read-only.

Software Management supports upgrading software images on RFF partitions by using a procedure called Rxboot upgrade. Before upgrading, reboot the device and put it into Rxboot mode, which makes the RFF partition available to write a new software image.

Q. When does Software Management use the remote copy protocol (rcp) to transfer images?

A. Generally the order defined in selected protocol list will be used for transferring (to upload and download) Cisco IOS® Soft wares. If RCP is in the top of the selected protocol list then RCP is used as the first protocol for image transferring on to the devices that support CISCO-FLASH-MIB.

Check the supported protocol list for the device to find out whether device supports RCP or not. Cisco Catalyst 5500/5000 switches and Cisco 700 series devices do not support rcp. Cisco IOS devices that do not support rcp include the Cisco 7000 series (route processor [RP]-based 7000 only) and MC3810.

All other Cisco IOS devices support the rcp protocol. Protocol order defined for the Config option in **Resource Manager Essentials > Admin > Config Mgmt** will be used for the Config option.

Q. How does Software Management ensure that file corruption does not occur during transfer?

A. Software Management computes the checksum of the image file. Then, Software Management compares this checksum to the checksum from the device after the copy of the image file to the device Flash.

Software Management also verifies the size of the file on the Flash. If either the size or checksum do not match, Software Management aborts the distribution and marks the job status as an error.

Q. After an upgrade, why does Software Management sometimes leave behind image files in the tftpboot directory?

A. Software Management removes the image files from the tftpboot directory after the upgrade unless the TFTP fallback job option is set. If the TFTP fallback option is set, Software Management uploads the image from the device and leaves the image in the tftpboot directory for fallback.

Software Management also modifies the boot system commands on the device to add a fallback command to boot from the original image on the RME TFTP server if the upgraded image does not boot.

Q. How much temporary space do you need during image distribution?

A. The amount of free space necessary depends on the image file size and the number of devices for simultaneous upgrade. If the TFTP fallback option is set, you need additional free disk space to keep the current image in the tftpboot directory. Both the tftpboot and temp directories use disk space.

Q. Is Cisco.com connection mandatory for Software Management?

A. Cisco.com connection is not mandatory for using basic Software Management functionality. Image distribution, library management, tracking software upgrade changes, and other functions can run without Cisco.com connectivity.

Cisco.com connectivity provides the additional benefits of obtaining images and their attributes from Cisco.com and viewing the status of outstanding bugs against the software images running on the devices in the network.

The following features of Software Management require Cisco.com connectivity:

- Adding image to Repository from Cisco.com. Software Management can import images for all supported devices.
- Distributing images directly from Cisco.com to devices, also called Recommend Images from Cisco.com. Without a Cisco.com connection, the Recommend Images screen Image list box will not show any images from Cisco.com when it creates the Distribute Images job.
- Cisco.com upgrade analysis.
- Cisco IOS image deferral processing.

Q. How does Software Management handle proxy environments?

A. Software Management uses HTTP protocol to communicate to Cisco.com about downloading images and their attributes. If you use an HTTP proxy for Internet connectivity, configure Proxy URL information in **Common Services > Server > Security > Proxy Server Setup**.

Q. Does Software Management support proxy with user authentication environments?

A. Yes, Software Management support proxy that requires user authentication.

Q. Why is the Cisco.com filter option on the Software Management Edit Preferences screen not provided for Catalyst or Cisco 700 Series images?

A. During the Distribute Images task, Software Management communicates with Cisco.com to obtain a list of applicable images and their attributes. Based on this information, Software Management recommends an image.

There are many Cisco IOS images available on Cisco.com, which can cause a substantial delay in retrieving image attributes from Cisco.com. Some of these images will not be relevant to the user. Software Management filters the amount of images being considered to make a more meaningful and manageable subset.

For Catalyst and 700 devices, fewer images are available on Cisco.com than for Cisco IOS; therefore, it is not necessary to filter the images.

Q. How come the Cisco.com filter option does not work in LS1010 devices?

A. Although LS1010 devices run Cisco IOS images, there are some differences in how the LS1010 images are released. LS1010 images do not follow the Cisco IOS-type image releases like general deployment (GD), limited deployment (LD), and early deployment (ED).

Therefore, Software Management cannot effectively filter LS1010 type images. Nor does Software Management filter Catalyst 8500 Series images.

Q. Can I configure Software Management to retrieve images from a Cisco.com mirror site rather than the main Cisco.com site?

A. No. Although the mirror Cisco.com sites contain the images, they do not store image attributes, such as minimum RAM and FLASH requirement. This information is available only from the main Cisco.com site at http://www.cisco.com.

Q. Why I cannot download crypto images?

A. Crypto images are available only to authorized Cisco.com users. All users can view the images during the Recommendation stage but only users with the right privileges can download the image. Make sure that the Cisco.com Login user configured in CiscoWorks has permission to download crypto images.

Q. How does Software Management verify the integrity of the images after importing them from Cisco.com?

A. Software Management checks the validity of the downloaded images by comparing the MD5 checksum of the image with the MD5 checksum value retrieved from the Cisco.com database.

Q. Why does the Flash size displayed in the Add Image to Repository (Source:Cisco.com) function not match the actual size for some Cisco IOS devices?

A. Software Management does not erase files whose sizes are less than 1 MB on Cisco IOS devices because those files may be config files that are backed up to Flash partitions or .html files or Java applets used for management.

Software Management subtracts sizes of all files whose sizes are less than 1 MB from the size of the Flash partition. The result of the subtraction is displayed as the size of the Flash partition in the Software Management user interface.

The Software Repository Management window (**Resource Manager Essentials > Software Mgmt > Software Repository**) displays the size of the largest Flash partition on the device. The size is displayed as an integer-truncated value in megabytes.

The Distribute Images screen displays information for all Flash partitions on the device. The values are displayed with two-decimal-digit precision.

The example below illustrates Software Management's behavior on a Cisco IOS device, which has two files whose sizes are 10 KB and 50 KB respectively.

The Flash card's total size is 8 MB. Because it has two files whose sizes are less than 1 MB, the Add Image to Repository screen displays the size as 7 MB. The Distribute Images screen displays the size as 7.94 MB.

```
enm-2502> show flash
System flash directory:
File Length Name/status
1 8089628 c2500-js-l.112-14.bin
2 10470 test_file1
3 52995 test_file2
8153288 bytes used, 235320 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Q. What is a Dual Flash Bank device?

A. The Flash card can be partitioned into two equal banks. Each bank is called a Flash partition. A Flash card that is not partitioned is Single Flash Bank (SFB) and the device is called an SFB device. A device that has its Flash card divided into two partitions is a Dual Flash Bank (DFB) device.

When Flash is partitioned into two separate banks, they are named flash1 and flash2. Software image files have to be completely stored in a single partition, so the maximum size of a software image is limited by the total size of any Flash partition.

On a Dual Flash Bank Run-from-Flash (DFB RFF) device, Software Management supports upgrading the flash partition that does not contain the running image. In other words, Software Management cannot upgrade the RFF partition on DFB devices.

This is because the other partition, which can be upgraded directly, is the recommended partition for storing the new software image.

The AS5200 device has two Flash cards, bootflash and flash. The flash is an RFF system and bootflash is an RFR system. The bootflash is intended for storing bootldr images on the AS5200 and flash is for storing Cisco IOS System Software.

Q. Does Software Management support software upgrades on dual RSP-based systems?

A. Software Management updates the software on the master RSP processor by copying the software image file to the master RSP Flash card (bootflash: slot0: slot1:) and updating the config file on the master RSP. Software Management cannot do a complete job of upgrading the software on the slave RSP processor.

Software Management can only copy the software image file to the slave RSP processor, but it cannot update the config file on that processor. Users will have to run a separate Distribute Images job to copy the software image file to the slave RSP processor.

Since Software Management cannot update the config file on the slave RSP processor, users must select **Don't touch config file** and select the No Reboot option in the job created for upgrading software on the slave RSP processor.

Q. Why does Software Management require static IP routes or dynamic IP routing protocol for configuration for the upgrade of a run-from-Flash (RFF) partition on a Single Flash Bank (SFB) device?

A. Software Management upgrades SFB devices that are in Rxboot mode. Rxboot mode does not support IP routing, IP bridging, or Simple Network Management Protocol (SNMP). The Rxboot image can support only one IP interface. Before the reboot of the device while in the Rxboot mode, Software Management determines the:

- Interface that connects the device to RME servers. Software Management shuts down all interfaces except the one that connects to the RME server.
- Default gateway IP address for the forward of all IP traffic when the device is in the Rxboot mode.
- Software Management queries the ipRouteEntry MIB variables ipRouteDest and ipRouteIfIndex to determine the default gateway IP address and the interface that connects.

If the device configuration does not include static IP routes or dynamic IP routing protocol, the ipRouteEntry table is not set on the device. Consequently, Software Management cannot determine the default gateway and the interface that connects to RME.

Q. Although the configuration of the Single Flash Bank (SFB) device includes an IP default gateway, why does Software Management not upgrade the device?

A. Software Management requires an IP default gateway address and an interface that connects. If you configure only the IP default gateway with the configuration command (ip default-gateway ip-address), you do not generate the ipRouteEntry MIB table on the device.

You can parse the IP default gateway from the configuration file; however, there is no reliable way to get the connecting interface from the device without the ipRouteEntry MIB. Without the ipRouteEntry MIB, Software Management does not allow upgrades, even if you have manually configured the IP gateway on the device.

Q. How do you change the IP default gateway configuration to allow Software Management to upgrade a device?

A. Use the IP default gateway configuration command to convert to a static IP route. Replace ip default-gateway gateway_ip_address with ip route 0.0.0.0 0.0.0.0 gateway_ip_address, which removes the ip default-gateway command from the configuration file. Check the output of the show ip route command to verify the correct configuration of a static IP route on the device.

Q. Why does Software Management require Cisco IOS Software Release 11.1 or later to run on a Single Flash Bank (SFB) device for an upgrade when you have configured the device with Frame Relay subinterfaces?

A. Releases earlier than Cisco IOS Software Release 11.1 do not include Frame Relay subinterfaces in ifTable and ipRouteTable in RFC 1213. Software Management requires information from these tables to perform Rxboot mode upgrades.

Therefore, Software Management requires Cisco IOS Software Release 11.1 or later to run on an SFB device when the device has Frame Relay subinterfaces.

Q. How is the job directory organized?

A. When Software Management schedules a job, it creates a new directory:

- On Solaris: /var/adm/CSCOpx/files/rme/swim
- On Windows, *NMSROOT*/files/rme/swim

  Where *NMSROOT* is the CiscoWorks installed directory.

  The directory name is the integer ID of the job. (Example: /var/adm/CSCOpx/files/rme/swim/23, where 23 is the Job ID.)

  The Job directory contains the following files depending upon the type of Software Management task:

Distribution Job	Image Import Job Image	Synchronization Job
• swim_debug.log • workorder.html • distribution.xml • PostOperation.txt • SwOperation.txt • SummaryTable.tab • Hostname.upgStatus • HostName_Config_Snap	• swim_debug.log • workorder.html • import.xml • PostOperation.txt • SwOperation.txt • SummaryTable.tab • Hostname.upgStatus	• swim_debug.log • workorder.html • synchreport.xml • jobinfo.xml • synchReport.txt

Where,

- swim_debug.log contains the debug information during the job execution.
- workorder.html contains the changes that user has chosen to perform with the job
- *deviceName*.upgStatus- a serialized file created on job completion for Retry and Undo options.
- PostOperation.txt used for all jobs scheduled through UI.
- SwOperation.txt indicates Job has been triggered. Absence indicate job has crashed for what ever reasons
- SummarTable.tab for UI purposes always exists for executed job.
- _Config_snap contains the Changes that are performed by Software Management on the original configuration.
- HostName_telnet.log for some device types only.

Q. Which modem cards does Software Management support?

A. Software Management upgrades Modem ISDN channel aggregation (MICA) and Microcom 56K modems.

Q. Which devices and software versions get support for the modem upgrades?

A. Support is available for Modem ISDN channel aggregation (MICA) portware upgrades on:

- Cisco AS5200 that runs Cisco IOS Software Release 11.3(2)T or later and Bootldr version 11.2(11)P or later.
- Cisco AS5300 that runs Cisco IOS Software Release 11.2(9)XA, 11.3(2)T, or later.
- Cisco 3640 that runs Cisco IOS Software Release 11.2(12)P, 11.3(2)T, or later.

  Support is available for Microcom firmware upgrades on:

- AS5200 that runs Cisco IOS Software Release 11.2(10a)P or later.
- AS5300 that runs Cisco IOS Software Release 11.1(14)AA, 11.2(7a)P, or later.

Note Cisco AS5800 devices also have modems. However, the modem microcode for these devices is bundled with the system software only and receives upgrades as part of the system software upgrade.

Q. Which formats of Microcom firmware images does Software Management support?

A. The Microcom firmware for 56K modems is available in two formats:

- Controller firmware and the Digital Signal Processor (DSP) code as two files, for example, mcom-modem-fw-xx.bin and mcom-modem-dsp-xx.bin.
- A combination of firmware and the DSP code in a single format, for example, mcom-modem-code-xx.bin.

The Cisco AS5300 supports only the image combination. If the Cisco AS5200 runs a Cisco IOS Software release later than Cisco IOS Software Release 11.2(10)P, the AS5200 supports only the combination file format.

Software Management supports only the combination format files (for example, mcom-modem-code-xx.bin). Software Management does not support separate firmware and DSP code files. You cannot import the files to the software library.

Q. Which format of Modem ISDN channel aggregation (MICA) portware do Cisco 3600 devices support?

A. The 3640 digital modem network modules can run two types of modem microcode.

- 3600-Specific Modem Microcode File—This file has a 3600-specific header and should have the characters c3600-mica in the file name. Software Management does not support such files.
- Cisco AS5300 Modem Microcode File—In Cisco IOS Software Release 11.2(12)P, 11.3(2)T, and later, the 3640 supports the AS5300 microcode files directly and the 3600-specific microcode files.

  The AS5300 microcode files have Executable and Linking Format headers that contain the version and other information about the image file. Even though the microcode file formats differ between the 3600 and the AS5300, the actual microcode that downloads to the MICA modems is the same.

Software Management supports only AS5300 format files. Therefore, the earliest Cisco IOS Software release that the 3640 supports is Cisco IOS Software Release 11.2(12)P.

Q. Why does the Undo option not receive support for modem upgrades?

A. To support the Undo option, Software Management must determine the version of software that runs and identify the image file on the device that corresponds. The image file must be present in the library or available on Cisco.com.

In the case of modem upgrades, Software Management cannot precisely determine the current software version on the modems in all cases. Moreover, different modems can run different software versions, which makes the undo process difficult to support.

Q. What connection mechanism does Software Management use for modem upgrades?

A. Software Management uses Simple Network Management Protocol (SNMP) to initiate the modem image file transfer to the device Flash. After Software Management copies the image to Flash, Software Management uses the Telnet interface to the device to run a command line interface (CLI) command that downloads the code to the modems. (The command is copy flash modem.)

Q. Does Software Management erase Flash for modem upgrades if there is not enough free space on Flash?

A. Yes, if the target Flash card does not have enough free space for the store of the new modem image, Software Management erases the target Flash. Software Management does not erase the Flash card if:

- The upgrade of the system software does not occur within the same job as the modem upgrade.
- The target Flash partition for the modem upgrade contains the current system software image.

Instead, Software Management prevents the modem upgrade on that Flash partition. On the Cisco AS5200, the bootflash card stores modem images, which can contain the bootloader image that currently runs.

If there is not enough free space to contain the new modem image, Software Management erases the bootflash card. Back up and restore bootloader images in the case that an erase of the bootflash is necessary for the upgrade of the modem image. Software Management issues a verification warning if Software Management needs to erase the bootflash.

Q. What is CIP?

A. CIP stands for Channel Interface Processor card. This interface card allows you to connect the Cisco 7000 router to IBM or IBM-compatible mainframes.

Q. Which devices support the Channel Interface Processor (CIP) microcode upgrade? What is the minimum software version necessary?

A. Software Management supports CIP upgrades on Cisco 7000 and 7500 routers that run Cisco IOS Software Release 11.1(1) or later.

Q. What is the minimum Channel Interface Processor (CIP) version that Software Management supports?

A. Software Management supports CIP version 22.0 at minimum.

Q. How can you import Channel Interface Processor (CIP) images to the Software Management library?

A. The Add Images function (**Resource Manager Essentials** > **Software Mgmt** > **Software Repository > Add**) does not support the import of CIP microcode images from Cisco.com.

a. Download the images to the file system on the RME server.
b. Select the Add option with source as File System to import them to the software repository.

   Software Management does not recommend the download of CIP microcode directly from Cisco.com for an upgrade.
c. Populate the software Repository with modem images before you run the Distribute Images function.

Q. Is there support for the Undo option for Channel Interface Processor (CIP) upgrades?

A. No, there is no support for the Undo option for CIP upgrades.

Q. What connection mechanism does Software Management use to upgrade Channel Interface Processor (CIP)?

A. Software Management uses the Telnet interface to the device to copy the CIP image to the flash. Software Management uses TFTP (via Simple Network Management Protocol [SNMP]) for the configuration upgrade to add the boot command to load CIP microcode.

Q. Does Software Management change the configuration file for the Channel Interface Processor (CIP) upgrade?

A. To load the new CIP microcode, the CIP upgrade process adds these configuration commands:

```
microcode cip flash new_cip_image_name

microcode reload
```

Q. Does Software Management supports CIP2?

A. Yes, Software Management supports CIP2 images for CIP supported device types.

Q. In which order does Software Management upgrade modules on a Cisco Catalyst 5500/5000 device?

A. Software Management upgrades the Supervisor Engine module on the device before other modules. Software Management upgrades the remainder of the modules in slot-number order. For example, Software Management upgrades the module on Slot 3 before Slot 5.

Q. Does the Supervisor Engine card reboot after the upgrade of all modules?

A. If you elect to reboot devices immediately after the upgrade of software, Software Management reloads the Supervisor Engine card. The reload of the card results in the reload of all modules, before the upgrade of software on other intelligent modules. This process supports instances in which the new module requires a newer version of Supervisor Engine software.

If you choose not to reboot the device after the download of software, you then must reload the Supervisor Engine module manually. You also should consider that software that you have newly loaded on a module may require new Supervisor Engine software.

If a new Supervisor Engine software is necessary, you should reload the Supervisor Engine module before you load the new software to the other intelligent modules (such as ATM, FDDI, and Token Ring).

For example, you may download 3.1(1) FDDI software and 4.1(1) Supervisor Engine software in a single job. The 3.1(1) FDDI software may require 4.1(1) Supervisor Engine software. Then, you must reset the Supervisor Engine module before you can upgrade the FDDI software. In such cases, you must have already chosen the Reboot Immediately option.

Q. Does Software Management determine if the newly deployed Supervisor Engine software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor Engine software supports all modules that are available on the chassis.

Usually, with the upgrade of Supervisor Engine software to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. However, you should check the release notes of the Supervisor Engine software or module software to be sure that the software versions are compatible.

Q. Does Software Management support the upgrade of software on redundant Supervisor Engine card-based systems?

A. The redundant architecture of Cisco Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor Engine automatically synchronizes all the data from the primary Supervisor Engine. No special processes are necessary.

Q. Does Software Management update the configuration file on Cisco Catalyst 5500/5000 devices during the software upgrade?

A. Software Management updates the configuration file on Catalyst 5500/5000 devices only when the device has a Supervisor Engine III card. Software Management updates the boot system commands and the config register value if necessary.

For Supervisor Engine I and II and other module upgrades, Software Management does not update the configuration file on the device. Instead, Software Management uses CISCO-STACK-MIB and TFTP to download the configuration file. Before Software Management changes the configuration file on the device, Software Management backs up the file to the Job Schedule directory.

The example below illustrates the Software Management update of the configuration file. Assume that a Supervisor Engine III card runs 3.1(1) software. Also, assume that the software image file is on slot0 with the name cat5000-sup3.3-1-1.bin.

The configuration file boot system commands before the upgrade are:

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```

Software Management has upgraded the software to 4.1(2). The new software image is on the same Flash card as cat5000-sup3-4-1-2.bin. Software Management then performs these configuration updates:

```
clear all boot system all
```

This removes all boot system commands on the device.

```
set boot system flash slot0:cat5000-sup3.4-1-2.bin
```

```
set boot system flash slot0:cat5000-sup3.3-1-1.bin
```

The update modifies the BOOT environment variable on the Supervisor Engine III card. You can display the environment values on the device is you issue the show boot command from the Supervisor Engine command-line interface (CLI).

The config register update occurs only if the least significant four bits of the config register are not all set to "1".

For example, if the current config register value is 0x10F (with the least significant four bits all 1s), Software Management requires no change to the config register. If the current config register value is, for example, 0x111 or 0x11A, Software Management modifies the config register to 0x11F. The action generates this command:

```
set boot config-register 0x11F
```

Q. Does Software Management determine if the Supervisor Engine has the minimum required RAM to run a new image?

A. Software Management uses the Minimum Required RAM field for the Supervisor Engine software image. You can set this field when you import the image into the library. If you do not input a value in this field, Software Management uses this matrix to determine the RAM requirement:

Image Type Software Version RAM Requirement

- I, II sup < 2.1(1) 4 MB
- I, II sup > = 2.1(1) & < 3.1(1) 8 MB
- I, II sup8 > = 3.1(1) & < 4.1(1) 8 MB (8 MB RAM image)

- I, II sup > = 3.1(1) & < 4.1(1) 16 MB
- I, II sup > = 4.1(1) 16 MB
- III sup3 > = 3.1(1) 32 MB

Images that are 8 MB RAM are available in 3.1 and 3.2 software releases only for Supervisor Engine I and II cards.

Software Management tries to use CISCO-MEMORY-POOL MIB to determine the available memory on a device. The MIB is implemented from 4.1(1) Supervisor Engine software (on all different Supervisor Engine card types—I, II, and III).

- If a device runs the software that implements this MIB, Software Management performs a memory check between the image requirement and the size of DRAM that is on the device.
- If the device does not have enough RAM to run the image, Software Management generates a verification warning.
- If the current software on the device is earlier than 4.1, Software Management generates a generic verification warning about memory requirements.

Q. Are there restrictions on the downgrade of the software on the Supervisor Engine card and other modules?

A. You can downgrade Supervisor Engine card software to version 4.1(1) or later.

For example, if a Supervisor Engine card runs 4.2(1) software, you can downgrade the software to 4.1(2) or 4.1(1). However, you cannot downgrade the same Supervisor Engine card to 3.2(1b). If a Supervisor Engine card runs 3.2(2), you cannot downgrade the software to 3.1(1) or 2.4(1).

There are no restrictions for the downgrade of software on other modules, such as ATM, FDDI, and Token Ring. However, you should check the release notes of new software before you attempt downgrades on modules.

Q. Do you need to reconfigure the device when you downgrade the Supervisor Engine software?

A. When you downgrade Supervisor Engine software, parts of the configuration may be lost. You must check the configuration file and reconfigure as necessary. Use the backed up Software Management configuration file from the Job Schedule directory as a reference, or use the backed up configuration file from the Config Archive.

Q. In the 4.1(1) software release and later, Supervisor Engine III cards allow the storage of configuration files on Flash cards. Does Software Management preserve the backed up configuration files on Flash during a software upgrade?

A. Software Management erases a Flash card on Supervisor Engine III if the free space on the Flash card cannot store the target software image. Software Management does not erase files of sizes that are less than 1 MB during software upgrades. Since configuration files generally do not exceed 1 MB, Software Management does not erase these files.

Q. Does Software Management allow you to upgrade epsboot images on Token Ring cards on Cisco Catalyst 5500/5000 devices?

A. Software Management does not allow upgrades of epsboot images on Catalyst 5500/5000 devices. An epsboot string in the file names can identify epsboot images. Epsboot upgrades are not often necessary. You can perform the upgrades with the Supervisor Engine card command-line interface (CLI).

Q. Why does the Add Image to Repository (Source: Cisco.com) task not display Token Ring LAN Emulation (LANE) or Permanent Virtual Circuit (PVC)-only ATM software images?

A. The Add Image to Repository (Source: Cisco.com) function in Software Management displays software images for only a subset of these ATM modules:

- WS-X5153
- WS-X5154
- WS-X5155
- WS-X5156
- WS-X5157
- WS-X5158

Software images for these modules have version numbers that range from 2.2 to 3.2(8).

The WS-X5153 to WS-X5158 modules can run:

- ATM LANE
- PVC Traffic Shaping
- Token Ring LANE software images

Software Management also supports the upgrade of software on these modules:

- WS-X5161
- WS-X5162
- WS-X5165
- WS-X5167
- WS-X5168

However, no mechanism exists to import the images from Cisco.com directly into the Software Management software library for these modules. The software images that run on the modules support LANE on Ethernet, Token Ring, and PVC traffic shaping.

You must download the software images for these modules directly from Cisco.com. Then, import the images into the library with the Add Image to Repository function.

Software Management does not support software management on WS-X5166 modules.

Q. How do you identify software image files for each of the ATM modules that Software Management does support? What are the file-name conventions on Cisco.com?

A. ATM software image file names and version numbers determine on which modules the software image can run and identify the features that receive support. This table provides details on version numbers and file-name conventions.

Q. How can I make the Image Recommendation faster?

A. If you select Cisco.com image recommendation, try to limit the images by filtering (**RME > Admin > Software Management > View/Edit Preferences**).

Module IDs	Image Feature/Version	Image File Name Format (Example)	Version to Input in Software Management
WS-X5153 to WS-X5158	Ethernet LAN Emulation (LANE) 2.2 to 3.2(7)	cat5000-atm.ver_number 3.2(7) cat5000-atm.3-2-7.bin	2.2-3.2(7)
WS-X5153 to WS-X5158	Ethernet LANE 3.2(8)	c5atm-wblane.Cisco *_IOS_Software_rel_number* c5atm-wblane.113-2.5.WA4.4m.bin	3.2(8)
WS-X5153 to WS-X5158	Token Ring LANE 70.x	c5k-trlane.*ver_number* c5k-trlane.70-1-1.bin	70.x
WS-X5153 to WS-X5158	Permanent Virtual Circuit (PVC) Traffic Shaping 50.x	cat5000-atm-pvcshape.*ver_number* cat5000-atm-pvcshape.50-1-1.bin	50.x
WS-X5153 to WS-X5158	PVC Traffic Shaping 51.x	c5atm-wbpvc.*Cisco _IOS_Software_rel_number* c5atm-wbpvc.113-2.5.WA4.5.x.bin	51.x
WS-X5161, WS-X5162, WS-X5167, WS-X5168 (Truckee)	Ethernet LANE, Token Ring LANE, PVC Traffic Shaping 4.3, 4.4	c5atm-wtall.*Cisco _IOS_Software_rel_number* c5atm-wtall.113-2a.WA4.4b.bin	4(3), 4(4b)

ATM version-number conventions differ for different classes of ATM images. PVC, Token Ring LANE, and Truckee types of ATM images have unique version-number conventions. Software Management recognizes the version numbers that appear in the last column of the table. The input of an incompatible version number results in upgrade job failures.

ATM software release notes give the original version number of the image as well as a version number that is close to the Software Management version-number scheme. Check the release notes for version-number schemes.

Q. Why do the software version numbers that the show module command output displays from the Supervisor Engine command-line interface (CLI) and the version numbers that Software Management uses fail to match in some cases?

A. ATM module software for Cisco Catalyst devices uses Cisco IOS Software code as a basis. The software release for Truckee ATM modules as well as ATM software releases 3.2(7) and later use the Cisco IOS Software version-number scheme.

Software Management does not recognize the Cisco IOS Software version-number scheme for Catalyst ATM software images. Use the simple version-number scheme that appears in the table in this document. (See the Version to Input in Software Management column.)

Output of the show module command of the Supervisor Engine CLI and the show command on the ATM module can display different versions. If the software that runs on the Supervisor Engine is earlier than 4.1, the Supervisor Engine software does not recognize the Cisco IOS Software version-number scheme of ATM images.

Therefore, the Supervisor Engine displays a different version number than the output of the show version command on the ATM module.

Q. Does Software Management recommend the right ATM image for your ATM module type?

A. Yes, Software Management distinguishes different flavours of ATM images and recommends images based on current class of ATM card on the device.

Q. Should you use special images with Software Management for Cisco Catalyst 2900XL/3500XL devices?

A. The 2900XL/3500XL devices have three images:

- Regular Cisco IOS Software image.
- A TAR format HTML image that contains files for Visual Switch Manager.
- A TAR format image that contains both these images.

Software Management uses the TAR format image that contains the Cisco IOS Software and HTML image. This image posts on Cisco.com, as do other images for 2900XL/3500XL.

When you use RME for software upgrades, you should use images with the description Enterprise-IOS and HTML-Use with RME 2.1 or later or Standard-IOS and HTML-Use with RME 2.1 or later. When you use Add Image to Repository from Cisco.com/Slam Dunk, you are able to see only these images.

Q. How does Software Management handle image import functionality of TAR and bin types of images for Catalyst 2900XL/3500XL devices?

A. For 2900/3500 device types Both .tar format and .bin format images are supported as system software. Network Synchronization option (Add image from network as source) will not be able import tar images because when the image downloads to the switch, the image distributes as small individual files on the flash in different directories.

The switch command-line interface (CLI) does not provide commands to combine all the files and make a new TAR file that Software Management can then upload. Whereas the .bin image can be imported from the device as well as from the Network Synchronization option.

Q. Why do software upgrades take longer on Cisco Catalyst 2900XL/3500XL devices?

A. Software Management uses command-line interface (CLI) to download software to 2900XL/3500XL devices. Because the software on these devices has many HTML/gif files on the Flash, the software must first delete all the files and then proceed with the new software download. Deletion of the images takes time, which is why software downloads to devices can take up to 20 minutes.

Q. How do you upgrade Route Switch Module (RSM) and LightStream 1010 (LS1010) module software on Cisco Catalyst 5500/5000 and 6500/6000 series switches?

A. The RSM (also called the VLAN router) on a Catalyst 5500/5000 or 6500/6000 switch and the LS1010 module on a Catalyst 5500/5000 switch run Cisco IOS Software. RSMs and LS1010 modules have individual IP addresses and Simple Network Management Protocol (SNMP) agents. The RME Inventory manages these modules as separate devices.

You can find the IP address of the RSM if you look at the Detailed Inventory report of the Catalyst 5500/5000 and 6500/6000 device that has the RSM on the chassis. The Module IP Address column in the Stack Modules section shows the IP addresses of all modules on the chassis.

If you do not find the addition of RSM or LS1010 to Inventory, you must first add the module as a device to Inventory before you attempt Software Management functions. Software Management functions that run on Cisco IOS devices also can run on an RSM or an LS1010.

Q. Why does the Distribute Images task show all the images from Cisco.com for LightStream 1010 (LS1010) and Cisco Catalyst 8500 devices, even though you have configured Cisco.com filtering?

A. Although LS1010 and the 8500 devices run Cisco IOS Software images, differences exist in the means of image release. The images do not follow the Cisco IOS Software image releases, such as general deployment (GD), limited deployment (LD), and early deployment (ED). Therefore, Software Management cannot effectively filter LS1010-type and 8500-type images.

Q. What is the minimum version that Cisco 700 series ISDN routers support?

A. For Cisco 760 Series ISDN routers, Software Management requires a minimum software version of 3.2(4) on the device. For Cisco 770 Series ISDN routers, the minimum version necessary is 4.0(1).

Q. What connection mechanism does Software Management use for Cisco 700 series upgrades?

A. Software Management uses the Telnet interface to the device to copy the 700 series image to the flash. Software Management uses TFTP protocol. The RME workstation is the TFTP client, and the device is the TFTP server.

Q. Both Cisco 760 and 770 series devices run the same image. Why do you see only some images with versions later than 4.0(1) for 770 series devices but see all images for 760 series devices?

A. When you load an image with a version earlier than 4.0(1) onto a 770 series device, the sysObjectID box changes to something other than Cisco-assigned. Also, RME identifies the device as a non-Cisco device. Therefore, Software Management does not list images with versions earlier than 4.0(1) for Cisco 770 series upgrades.

Q. Why do you not see the option to reboot the device later on the Job Control page for Cisco 700 series routers?

A. There is no option to reboot the device later because 700 series routers reboot at the time of the new image download.

Q. Why do you not see the option to modify the boot commands on the Job Control page for Cisco 700 series routers?

A. Only one image at a time can appear on the 700 series devices, which means the boot command does not apply to these devices.

Q. Why does Software Management report download failures for some images even though the device runs the new image after the job completes?

A. Some new Cisco 700 series images use nonstandard name convention or nonstandard versions. Software Management incorrectly parses the version number from file names of those images. After the download of the new image, the device reboots.

Software Management retrieves the new image version from the device and compares that with the version that Software Management parsed. The two versions do not match. As a result, the software download appears to have failed, which generates as an error.

This problem occurs with c760-in.b-US.42-3.5.bin and c760-in.b-US.43.1.bin images for all countries.

You can resolve this issue by entering the correct version number when you import the image from the file system.

For example, for c760-in.b-US.42-3.5.bin, enter 4.2(3.5). For c760-in.b-US.43.1.bin, enter 4.3(1) as the version number.

Q. In which order does Software Management upgrade modules on a Catalyst 5000 device?

A. Software Management upgrades the Supervisor module on the device before other modules. The remainders of the modules are upgraded in the order of their slot number. For example, the module on Slot #3 is upgraded before Slot #5.

Q. Does Software Management check to see that the newly deployed Supervisor software or module software is compatible with the module types (or module hardware versions)?

A. Software Management does not verify whether the newly deployed Supervisor software supports all modules that are available on the chassis.

Usually, when Supervisor software is upgraded to a newer release, the software provides backward compatibility for all the modules that exist on the chassis. Users are encouraged to check the release notes of the Supervisor software or module software to make sure that the software versions are compatible.

Q. Does Software Management support upgrading software on redundant Supervisor card-based systems?

A. The redundant architecture of Catalyst devices ensures that when the device reboots after a software upgrade, the redundant Supervisor automatically synchronizes all the data from the primary Supervisor. No special processing is required.

Q. What is the purpose of user scripts?

A. User-supplied scripts are run before and after each device upgrade. They can be used for pre- and post validation checks. For example,

- The pre-upgrade script can check whether the device is accessible.
- The pre-upgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before proceeding with the upgrade.
- The post-upgrade script can check whether the device has upgraded successfully or not. Depending on the return value, Software Management either halts or continues with the rest of the upgrade job.

See Understanding User-supplied Scripts section in Chapter 12: Managing Software Images Using Software Management in the *User Guide for Resource Manager Essentials 4.1* for more details on Software Management script.

Q. What if the user script crashes? Will it crash the Software Management job also?

A. No, crashing of the script will not stop the Software Management job. Software Management executes the script in a different process space so the script crashing will not crash the Software Management job. But Software Management will assume the script has failed.

Q. When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?

A. There are two options that import images from the network to the Software Repository:

- Baseline tasks
- Synchronization

The baseline task (**Resource Manager Essentials** > **Software Mgmt** > **Software Repository** > **Add** > **Network**) should be done only once as a part of the initial setup. This imports the images running on the network to your Repository.

To keep the Repository synchronized with any new images and changes caused by upgrades from sources other than Software Management, schedule a synchronization job to run periodically at appropriate intervals.

When this synchronization job runs, it looks for differences between the Repository and the network and allows any new images to be imported. During job distribution, Software Management backs up the current running image only if the option, Use current running image as tftp fallback image was selected when the job was created.

Q. Can I set up a periodic download of Software Management images from Cisco.com?

A. No. However, you can schedule a one-time import from Cisco.com to occur at a later time. Software Management does not allow you to automatically import images from Cisco.com to the Repository based upon your preferences.

Q. Is browser timeout something I should consider when downloading?

A. The Image Import option from Cisco.com and other devices can be done on a scheduled basis. Since this process runs as a background task on the server, the browser is not involved. However, when an Immediate Import job runs, it is performed as a foreground task, and the browser can still timeout.

Q. What are crypto images?

A. Crypto images are software images that use 56-bit Data Encryption Standard (DES) (or higher) encryption, and are subjected to export regulations. You must be a registered Cisco.com user, and be eligible and authorized to download such images.

Q. How much temporary space is required during image distribution?

A. The amount of free space that is required depends upon the image file size and the number of devices that are being upgraded simultaneously. If the **`tftpfallback`** option is set, additional free disk space is required to keep the current image in the tftpboot directory. Disk space is used both in the tftpboot and temp directories.

Q. At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?

A. The software images directory gets created at the time of importing an image to the Repository; however, this should be transparent to you.

Q. How can I speed up Image Recommendation?

A. If you include Cisco.com for Image Recommendation, try to limit the images by filtering (**Resource Manager Essentials** > **Admin** > **Software Mgmt** > **View/Edit Preferences**).

Q. When a job is rejected, can it be edited or should I resubmit?

A. No. You cannot edit or retry the rejected job. You should schedule a new job.

Q. Can different group members edit jobs? What are the restrictions?

A. The only job attribute that can be edited is the schedule time for non-Job Approval jobs. Any user who has the *Network Administrator* role defined can edit jobs or create new jobs; however, in the Job Approval model, the jobs can only be approved by users who are in the approver list specified during the creation of the job.

Q. What is the role of the registry files in RME?

A. Software Management manipulates the Windows registry to automatically manage remote authentication during the **rcp** transfers on Windows. The following registry parameters are important for **rcp** service on Windows:

- *HKEY_LOCAL_MACHINE\SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\DEBUG

  Dictates the amount of debug information written in the Windows event log.
  (Default = 0, Maximum = 0xff)

- *HKEY_LOCAL_MACHINE\SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\rhosts

  Contains the list of authenticated hosts that can run remote commands on this machine. This list is automatically managed by Software Management.

- *HKEY_LOCAL_MACHINE\SYSTEM*\CurrentControlSet\Services\crmrsh\Parameters\rusers

  Contains the list of authenticated remote users that can run remote commands on this machine. This list is automatically managed by Software Management.

- H*HKEY_LOCAL_MACHINE\SYSTEM*CurrentControlSet\Services\crmrsh\Parameters\NoRuserCheck

  If set to 1, the remote user authentication is skipped or, in other words, any remote user from authenticated hosts can run commands on this machine. (Default = 0)

- *HKEY_LOCAL_MACHINE\SYSTEM*CurrentControlSet\Services\crmrsh\Parameters\NoRhostCheck

  If set to 1, the remote host authentication is skipped or, in other words, commands can be run on this machine from any remote machine.
  (Default = 0)

Q. How do I upgrade Network Analysis Module (NAM) using Software Management?

A. To upgrade NAM using Software Management:

- Ensure that the passwords for NAM's application and maintenance modes are the same.

  This is because Software Management takes the password information from Inventory. However, Inventory requires the application mode password to manage the device, and Software Management requires the maintenance mode password to upgrade the device. Therefore, the passwords for NAM's application and maintenance modes should be the same.

- For a NAM card present in a Catalyst 6000 device running CatOS, ensure that you set auto logout to a value that is high enough to allow the copying of the new image.

  This is because a NAM image is usually very large (nearly 65 MB), and it may take between 1 to 2 hours to copy this image during Software Management upgrade. We recommend that you set the auto logout to 0 to ensure that there is no auto logout while the image is being copied.

  To set the auto logout value, use the CLI command, **`set logout 0`**.

  For a NAM card present in a Catalyst 6000 device running IOS, ensure that you set exec timeout to a value that is high enough to allow the copying of the new image. We recommend that you set the exec timeout value to 0 (**`exec-timeout 0 0`**) on all the vty lines.

- Ensure that the htdocs directory under CSCOpx has enough space to stage the NAM image.

  During the NAM upgrade, Software Management first copies the NAM image from the *NMSROOT*/CSCOpx/files/sw_images directory, to the *NMSROOT*/CSCOpx/htdocs/swimtemp directory and then copies the NAM image to the NAM card, using HTTP.

- Ensure that NAM is added with the correct Local User (root) and its password.
- Ensure that NAM is added with the correct SNMP read/write community strings.

- Ensure that the switch, which contains NAM, is added with the correct attributes.

Q. Can I change the job scheduled time?

A. The job scheduled time can be modified only for pending jobs that do not require approval.

For a job that requires approval, you must cancel the job and retry or recreate the job.

Q. How does Software Management handle the job status for an abnormally terminated job?

A. Software Management checks the last modification time of the job results file for each running job when the Browse Job Status screen is displayed. If the results file has not been modified for the last six hours, Software Management assumes that the job was terminated abnormally (server reboot is a probable cause for the termination), and the job status is changed to Error.

Q. How does Software Management handle the job status of a pending job whose scheduled time has passed?

A. Software Management checks the scheduled time for each pending job when the Browse Job Status screen is displayed. If the current time is an hour past the scheduled time for starting the job, (lack of operating system resources is a probable cause for the job not running at the scheduled time), the job status is changed to Error.

Q. Why are some files left in the Software Management folder after Software Management has been uninstalled?

A. When uninstalled, Software Management does not remove the software images directory from the RME server. The software images directory contains subdirectories for storing software images for various device families.

Q. **How can I enable or disable the SSH to Telnet fallback for RME - Software Management jobs?**

A. To enable or disable SSH to Telnet fallback for RME Software Management jobs:

Step 1 Go to **RME** > **Admin** > **Software Mgmt** > **View/Edit Preferences**.

Under the Distribution pane, there is a checkbox option, **Use SSH for software image upgrade and software image import through CLI (with fallback to TELNET)**.

Step 2 Do either of the following:

- Check this option, to enable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.
- Uncheck this option, to disable the use of SSH for software image upgrade and software image import through CLI along with fallback to Telnet.

Step 3 Click **Apply to save your changes.**

Q. **How can I export the images from RME-SWIM repository to a local drive or a file system mounted to the RME server?**

A. To export the image from RME Software Repository to a local drive or a file system:

Step 1 Select **Resource Manager Essentials** > **Software Mgmt** > **Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select images that you want to export, then click **Export**.

A confirmation message appears, `The selected images will be exported`.

Step 3 Click **OK**.

The Select directory to export window appears.

Step 4 Click on **Browse** to select a directory to which you want to export the selected images.

The Server Side File Browser dialog box appears.

Step 5 Choose the required directory and click **OK**.

The Image Directory field in the Select directory to export window displays the directory location which you had selected.

Step 6 Click **Next**

A progress bar appears indicating the progress of the export of images.

The Export Image(s) Summary Report appears after completion of the export of the image(s) with these details:

- Number of Selected Image(s)
- Target Directory
- Summary

Step 7 Click **Finish**.

You have successfully exported the image(s) to the selected directory.

Q. Does flash get erased if there is no sufficient space for Patch Distribution?

A. No. Patch Distribution requires sufficient amount of free space in flash and so it cannot be erased.

Q. When I try to copy images, the Image Copy option fails indicating that the External TFTP server is inaccessible.

A. If you come across this error, try any of these:

- Check whether TFTP service is running or stopped in the External TFTP server. If stopped, start it.
- Check if any security agent is preventing the application. If so register the application with security agent or disable the security agent.

Q. No information is logged in the log file for Software (SWIM) CLI.

A. Check the log level settings for CLI framework under:

Resource Manager Essentials > Admin > Application Log Level Settings and ensure that Logging Level is set properly.

Q. Can I specify the name of my input file as imagenames.txt when I try to export images using the Software Management (SWIM) CLI `exportimages` command?

A. Do not name your input files similar to arguments.

For example, if you specify

```
cwcli swim exportimages -input imagenames.txt -u admin -p admin
```

the following error message will be displayed

```
Invalid argument: imagenames
```

For example, you can specify the input filename as sample.txt

You can enter the following argument in your sample.txt

```
-imagenames image1,image2,image3,image4..........
```

So the exportimages command with input file will be:

```
cwcli swim exportimages -input sample.txt -u admin -p admin
```

Troubleshooting Software Management

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0013	Image Import option not supported for the selected device(s)	Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.	None.
SWIM0014	No images to import into library from the selected device(s)	Either: • There are no images on the Flash Or • Cannot get Flash information from inventory.	Check the Inventory Detailed Device Report to ensure that Flash file information exists for the device. If report generation fails, schedule an inventory collection job and redo the Software Management image import job.
SWIM0019	Could not perform Image recommendation for the selected device(s) because of insufficient data.	Could not fetch Image information from the Inventory database.	Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device. If report generation fails, schedule an inventory collection job and perform Software Management recommendation.
SWIM0020	Image Import option not supported for the selected device(s)	Image Import option is not supported because of device limitations. Check Software Management feature support matrix against the selected device platform.	None.
SWIM0021	Error encountered while parsing Job Data.	Either the Job Data file could not be located or the data for Image Upgrade was not provided.	Check whether you have access permissions to Job Directory, or re-create the job. If the problem persists, send all log files under job directory to TAC.
SWIM0027	Staging of the Image on the Remote Stage Device failed.	Image Copy to Remote Stage device failed because of SNMP Agent problems during transfer.	Check for any known bugs against the Image running on Remote Stage, or choose a different device. If the problem persists, send all log files under job directory to TAC

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0028	Cleanup option on Remote Stage Device failed.	Image Erase or a Configuration download caused an error.	Check for any known bugs against the Image running on Remote Stage.
SWIM0034	Device reboot failed.	Either: • The device configuration for reboot is missing Or • The image downloaded onto the device is not suitable for the device to come up.	Check whether the **snmp-server shutdown** command is configured on the device. You can do any of the following: • Configure the devices and re-schedule the jobs. • Use NetConfig reload template to reload the devices. • Reload manually if you have only a few set of devices.
SWIM0036	Image addition to Software Library failed	Either an invalid image was imported into library or the image is corrupted.	Check whether the image is downloaded completely in the directory
SWIM0056	Invalid Remote Stage device selected.	Cannot use this device as Remote stage because of device limitations.	Check the Help documentation to see which devices can be used as Remote Stage.
SWIM0067	System software analysis failed	This is an unexpected runtime error.	contact Cisco TAC.
SWIM0089	Could not perform Image Import from Cisco.com on the selected device(s).	Add Image from Cisco.com not supported for the device. This is because Cisco.com could not find the device platform in the supported list.	Check the Software Management feature support matrix against the selected device(s) platform.
SWIM0092	Could not perform Image Import from Cisco.com on the selected devices because of insufficient data.	The device information needed to fetch images from Cisco.com does not exist in Inventory.	Check the Inventory Detailed Device Report to ensure that Chassis information exists for the device. If Chassis information is missing, schedule an inventory collection job and retry the import workflow.
SWIM0093	Could not get Image information from Cisco.com	Could not connect to Cisco.com from CiscoWorks Server either because of incorrect Cisco.com credentials or missing proxy configuration.	Check whether Cisco.com credentials are correct. If they are correct, check whether the proxy server is configured with right proxy credentials. To configure proxy, go to: CiscoWorks Home page > Server > Security > Proxy Server Setup.
SWIM0101	The current version of the image on the device is different from the earlier version of the image.	This message is displayed when you retry a failed distribution job. This mainly happens when other jobs change the current running image of this device before scheduling the retry.	Try a new distribution job instead of retrying.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0118	Software Management application could not verify the inputs since there was no running image information. The device package may not have been installed. You can install it now and retry the task or you can install it before running the job. However, the results may not be accurate.	Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by RME.	Schedule the distribution job for a future date when the device is deployed Otherwise, the device package for this unsupported device will be installed and available in the RME server.
SWIM0119	Software Management application could not verify the flash inputs since there was no flash information available. Edit the expert input file and verify it again. If you do not want to edit the expert input file, you can continue with the task by clicking Next. However, the results may not be accurate.	The selected device does not have any Flash related information. Generally the flash details are present in the Inventory. You can check the Detailed Device Report to see the flash details. If there are no flash details for this device, Software Management will allow the user to schedule a distribution job without verifying the flash details.	None.
SWIM0120	Software Management application did not verify the inputs since there was no running image information. If you find that the device package is not installed, install it before running the job. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	Advanced Distribution Flow: Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by RME.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the RME server.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0121	Software Management application did not verify the Flash inputs as there was no Flash information. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	The selected device does not have any Flash related information. Generally the flash details are present in the Inventory. You can check the Detailed Device Report to see the flash details. If there are no flash details for this device, Software Management allows a user to schedule a distribution job without verifying the flash details.	None.
SWIM0122	Software Management application could not verify the inputs since there was no running image information available. Update your inventory and retry the task. If you do not want to update the inventory, you can continue with the task by clicking **Next**. However, the results may not be accurate.	Either: • The selected device is not yet deployed in the network (pre-provisioned device) Or • It is still not supported by RME.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the RME server.
SWIM0123	Software Management application could not verify the inputs since there was no running image information. Update your inventory and retry the task. The image distribution will proceed based on the unverified inputs. However, the results may not be accurate.	Advanced Distribution Flow: The selected device is not yet deployed in the network (pre-provisioned device) OR Still not supported by RME.	Schedule the distribution job for a future date when the device is deployed. Otherwise, the device package for this unsupported device will be available and installed in the RME server.

Message-ID	Error Message	Probable Cause	Possible Action

SWIM0125	An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.	None.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris:
			`/var/adm/CSCOpx/log/swim_debug.log`

SWIM0126	An unexpected error has occurred. Contact Cisco support and attach the swim_debug.log file.	None.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris:
			`/var/adm/CSCOpx/log/swim_debug.log`

SWIM0138	Cannot connect to the Job Manager. Check whether the jrm process is running properly. If it is not running, restart it and try scheduling the job again.	None	To check whether jrm is running, run command: **`pdshow jrm`** If jrm is down, restart CiscoWorks.
SWIM0139	Running image information is not available in Inventory for Remote-Stage device *Devicename*. Perform Update Inventory and check whether the required Flash data appears in the Detailed Device report. If it appears, retry the job; else, the data is not yet available from the device.	Either: • The Inventory is not updated Or • The image device running on the device is not populating the required Flash MIB information.	If data is not available from the device (due to bug in the image), upgrade the device with the higher version image. This higher image populates the Detailed Device report with the required Flash data.
SWIM0141	There is not enough free space on the repository to store the selected files. Please free up some disk space and retry the job.	Disk space is not sufficient on the server.	Free up some disk space and retry the job.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0142	RepositoryException while checking for disk space.	Disk space is not sufficient on the server.	Free up some disk space and retry the job.
SWIM0146	Could not get active image information. Either the device is not reachable or the sysconfigName OID information is not provided by the device.	A distribution job scheduled using Advanced flow for pre-provisioned devices has failed and you have tried a Retry task on this job. The pre-provisioned devices does not have running images and so this error message is displayed.	Ensure that the device is deployed or the device package for this device is installed before a distribution job is run on this device.
SWIM1001	The input parameters to the Image Distribution/Image Import/Image Activate are invalid.	You may have used incorrect Device Data for this task.	Check the application log file for more details.
SWIM1002	An error occurred in staging Image *Image Name*.	There may not be correct permissions for the image in the software repository or for the directories required for staging.	Retry the Image Upgrade option.
SWIM1003	SNMP Agent does not support the required instrumentation to get information about the Flash File system.	The SNMP Agent on the device does not support CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB.	Check for any known bugs related to these MIBs for the image version running on the device.
SWIM1004	Cannot get details about the Flash File system on the device.	There may be a faulty implementation of the MIB on the device.	Check the Bug Toolkit application for any known issues on the running image version.
SWIM1005	Flash Device or Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Device or Partition is invalid.	Trigger inventory collection on the device.
SWIM1006	Flash Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Partition is invalid.	Update the inventory collection on the device.
SWIM1007	You have specified the storage location on the device in an invalid format.	None.	Enter a valid format. For example: [moduleNumber\]flashPartitionName:[partitionNumber]:filename In case of Andiamo devices: flashDeviceName://flashPartitionName/filename

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1008	You have specified an invalid format for the destination storage location.	None.	Enter a valid format. For example: `[`*moduleNumber*`\]`*flashPartitionName*`:[`*partitionNumber*`]:`*filename* In case of Andiamo devices: *flashDeviceName*`://`*flashPartitionName*`/`*filename*
SWIM1009	Inventory reported enough space on Flash partition, but the distribution task found that the space is insufficient and requires erasure. The distribution task is being terminated.	The inventory data may be stale.	Update the inventory for the device and retry the job.
SWIM1010	The size of the partition selected to copy the image, is less than the image size.	None.	Select another partition to copy the image.
SWIM1011	Destination file size on storage location and the source file size are different.	This may be because of a network problem or a bug on the device.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1012	The file copied on the destination storage location is invalid.	The File Copy may have failed because of temporary network errors.	Retry the File Copy option.
SWIM1013	You have specified an invalid Job directory.	The destination directory that has been specified to copy the configuration file from the device is invalid.	Check whether the destination directory exists. If the directory exists, check whether there are write permissions. Also check whether there is enough disk space.
SWIM1014	Cannot generate configuration changes for Remote Stage option.	None.	Check for file permissions on the Job directory.
SWIM1015	Cannot generate configuration changes for activating the device.	None.	Check for file permissions on the Job directory.
SWIM1016	Cannot load new configuration to Remote Stage Device.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1017	Cannot fetch configuration file from the device.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1018	Cannot upload new configuration to the device during image activation.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the task.
SWIM1019	Cannot reload the device. Device is not responding after the Reload command.	The image upgraded on the device has some issues.	Check the Bug Toolkit application for any known issues on the upgraded image version. Manually restore the device through the console.
SWIM1020	The device is not running the new image.	This may be because the new image is invalid or corrupted and the device has booted from another image.	Check the Bug Toolkit application for any known issues on the upgraded image version.
SWIM1021	Cannot get the IP Address of the server.	The DNS resolution of the RME server may have failed.	Enable DNS resolution.
SWIM1023	Distribution task is not supported for this device.	The device packages that are installed may not be the correct package.	Check whether the correct device packages are installed on the server.
SWIM1024	Either the file already exists in the directory or the system cannot create this file.	Check whether another file with the same name already exists in the directory, or check whether there is enough disk space.	Create disk space and retry the task.
SWIM1025	The Configuration Register on the device does not allow you to boot the image from Flash.	The Configuration Register is not set to value 0x2102.	Change the Configuration Register on the device and retry the job.
SWIM1026	Cannot create a file and store the modified configuration.	There may not be sufficient permissions for the application to create the file, or there may not be enough disk space.	None.
SWIM1027	Error while fetching inventory information.	The data required for the selected task is either incomplete or missing in Inventory.	Check whether the Inventory data exists for the device in the Inventory Detailed Device Report. If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.
SWIM1029	Cannot get the required inventory information for the device.	Either there was no inventory collection for the device or the device is not responding.	Update inventory for the device and retry the task.
SWIM1030	This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash.	Either the inventory has not been updated or the Flash file is deleted from the Flash.	Update the inventory and retry the task.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1031	No Candidate Images found for the running software.	Either: • Cisco.com is not included in the admin preferences Or • There are no applicable images in the software repository or Cisco.com	Check Admin preference or add images to software repository.
SWIM1032	Images obtained for Recommendation do not meet the hardware and software requirements of the selected device.	Either: • The Candidate Images were filtered based on the selected Admin Preferences Or • They did not meet the Flash/RAM/BootROM needed to run on the device.	Check the Admin Preference or add more images to software repository and retry thejob.
SWIM1033	Cannot find the Best-fit image for the device by applying compatibility checks.	Either: • The Candidate Images were filtered based on the selected Admin Preferences Or • They did not meet the Flash/RAM/BootROM needed to run on the device.	Check the Admin Preference or add more images to software repository and retry the job.
SWIM1034	No applicable images found for the device from the configured image sources.	Either: • Cisco.com is not included in the admin preferences Or • There are no applicable images in the software repository or Cisco.com	Check the Admin Preference or add more images to software repository and retry the job.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1035	Error while performing Recommendation option. Runtime error encountered while filtering images caused by a problem with a running image on the device.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1036	Runtime error while performing Recommendation.	None.	Retry the job.If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1037	Error while fetching Flash Partition information.	Either: • The Flash information cannot be got from Inventory Or • There is a problem with the running image on the device.	Update the inventory and retry the task. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1038	No Read-Write Partition found on the device.	None.	Install a flash device with a read-write partition and update the inventory.
SWIM1039	No Storage Recommendation is made for the device.	The selected device may not have sufficient free size partition to copy the image.	Check whether the selected device has the sufficient free size partition to copy the image.
SWIM1040	Cannot get the Flash information for the device.	Either: • The Flash information cannot be got from Inventory Or • There is a problem with the running image on the device.	Perform Inventory Collection and check whether the Flash information appears in the Detailed Device report. If so, retry the job. Else, data is not available from the device.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1041	This device upgrade requires opening an SSH/Telnet connection to the device.	Enable password is not configured correctly in Device and Credential Repository.	Make sure that the appropriate SSH/Telnet passwords are configured correctly in Device and Credential Repository.
SWIM1042	The amount of Bootflash on the device may not be enough to run the selected image.	The amount of Bootflash on the device may not be enough to run the selected image.	Specify the Bootflash size for the image by editing the attributes of the image stored in the software repository, increase the Bootflash size for the device, or select a different image for upgrading.
SWIM1043	Runtime error while performing Bootloader image verification.	Selected image version may not be in the standard version format.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1044	Bootflash partition will be erased before copying new image.	Selected Bootloader image does not fit in available space on Bootflash.	Select a different Bootloader image if available.
SWIM1046	Selected software does not fit in selected Flash partition.	Selected software image does not fit in the available space on Bootflash.	Select a different Flash partition for upgrading.
SWIM1047	Minimum software version required for MICA image upgrade is not known.	None.	Select the image in the software repository and update the minimum system software version using View/Edit Image Attributes option.
SWIM1048	The system software that is active on the device, cannot run the selected image.	The system software that is active on the device, is not compatible with the selected image.	Select a different image that can be upgraded with the current system software or upgrade the system software to *Software Version.*
SWIM1049	The selected image requires Flash to be erased during image upgrade.	None.	Check whether you have performed the necessary backup.
SWIM1050	Read-Write SNMP community string is not in the Device and Credential Repository.	The Read-Write SNMP community string is not available in the Device and Credential Repository.	Add Read-Write community string for the device in the credentials repository.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1051	Credential information cannot be obtained for the device.	Either: • The device is not managed in the RME server Or • The device credentials are not correct or the device access privileges are insufficient.	None.
SWIM1052	Enable password is not configured for the device.	For Run For Flash (RFF) partition software upgrades, the Enable password must be configured.	Configure the Enable password in the credentials repository.
SWIM1053	Selected MICA Image is the same as the running image on the device.	The software version of the image is the latest on the device.	None.
SWIM1054	Error while checking the Telnet credential of the device.	None.	Make sure that the Telnet credentials for the device are correct.
SWIM1055	Selected Flash partition is ReadOnly.	Either the Flash partition is not write-enabled or the Read-Write partition does not exist.	Check whether the Read-Write partition exists. Set the Flash partition to be write-enabled.
SWIM1056	The method to update the software on the selected storage device is unknown.	None.	Select a different Flash partition, if available.
SWIM1057	The device will be put into Rxboot mode for the image upgrade.	None.	Select a different Flash device for the system software, if available.
SWIM1058	The selected software version has some known problems in the Flash MIB options which will make this application unable to perform software upgrades on the device.	None.	Upgrade the device manually or select a later software version, if available.
SWIM1059	Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image.	The Router shelf software image is not compatible with the Dial Shelf software image.	See the Release Notes for the Router Shelf software image to make sure the current Dial Shelf software is compatible. If not, upgrade the Dial Shelf software.
SWIM1060	Cannot obtain the file size of the selected image.	The selected image may have been removed from Cisco.com.	Select another image for upgrading.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1061	Image available at Cisco.com is selected for upgrade. This image will be imported from Cisco.com when the job is run.	None.	Verify that connectivity to Cisco.com is available when the job is scheduled to run or select an image from the software repository.
SWIM1062	Selected image is already running on the device.	None.	Verify that this is the image you want to upgrade for the device. If so, no action is required. If this is not the image you want, select a different image.
SWIM1063	Minimum RAM requirement of the selected image cannot be determined.	RAM available on the device may not be enough to activate this image.	Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.
SWIM1064	RAM available on the device may not be large enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Select a different image or upgrade the RAM on the device and retry Upgrade.
SWIM1065	RAM available on the device may not be enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Specify the RAM size for the image by editing the attributes of the image stored in the software repository, increase the RAM size for the device, or select a different image for upgrading.
SWIM1067	Runtime error while performing verification of the selected image.	None.	Select a different image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1063	Minimum RAM requirement of the selected image cannot be determined.	RAM available on the device may not be enough to activate the selected image.	Update the minimum RAM value using View/Edit Image attributes or make sure that the device has enough RAM to activate the selected image or select a different image.
SWIM1068	Selected image does not have the minimum system software version required for the upgrade.	Selected image does not have the minimum system software version required for the upgrade.	Select a differ rent image with a version higher than 11.0.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1069	Feature subset of the running image cannot be determined. Select a different image.	This is a wrong message due to a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.	None.
SWIM1070	Feature subset of the running image cannot be determined. Select a different image.	This is a wrong message due to a bug. The correct message is: Feature subset of the selected image is a subset or equal to running software feature set.	None.

SWIM1071	System software analysis failed.	Some unknown error has occurred during image analysis.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris:
			`/var/adm/CSCOpx/log/swim_debug.log`

SWIM1072	Boot loader analysis failed.	Some unknown error has occured during analysis of the image.	Please contact Cisco TAC with the UI log available under:
			Windows:
			`CSCOpx\logs\swim_debug.log`
			Solaris:
			`/var/adm/CSCOpx/log/swim_debug.log`

SWIM1074	The selected image does not have any requirement to be analyzed. The image can be used to upgrade the device.	None.	None.
SWIM1075	Cannot find an image that is newer and can fit on the Bootflash.	None.	Add Bootloader images, to the Software Repository, with version greater than the running image version and that can fit into the Bootflash. Then retry the job.
SWIM1076	Cannot find a Read-Write Boot partition on the device.	Read-Write Boot partition is not available on the device.	Insert a read-write Bootflash on the device and update the inventory.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1077	Cannot find a Bootflash partition for the Bootloader image.	Bootflash partition is not available for the Bootloader image.	Insert a read-write Bootflash on the device and update the inventory.
SWIM1078	System and Bootloader images are getting upgraded to the same Flash partition.	System and Bootloader images are getting upgraded to the same Flash partition.	Select individual partitions for both, if available.
SWIM1079	Image version cannot be compared.	The image formats of both the images may not be compatible for comparison.	Check the format of the version. Select a different image for upgrading.
SWIM1080	Read-Write partition exists but you have selected the ReadOnly partition.	You may have selected Read only partition instead of Read - Write partition.	Select the Read-Write partition for upgrading.
SWIM1081	You have selected the Compressed System Image for Run From Flash (RFF) Upgrade.	Wrong image selected for Upgrade.	Select the correct image.
SWIM1082	Runtime error while comparing Modem Image.	Either a wrong modem image is selected for comparison or the modem image formats or not compatible.	Select a different Modem Image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1083	Cannot find an image that is newer and fits in the Flash.	None.	Add another image into software repository and retry the task.
SWIM1084	Cannot find a Minimum Flash Requirement for the device.	The Flash space available on the device may not be sufficient for the selected image.	Check whether the image fits on the device.
SWIM1085	The MinFlash Attribute is unknown for the selected image.	The selected image does not fit on the selected partition.	Check whether the image fits on the selected partition or select a different image.
SWIM1086	Device not supported.	The required device packages may not be installed on the server.	Check whether the appropriate device packages are installed correctly on the server.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1087	Cannot get the device representation.	The required device packages may not be installed on the server.	Check whether the appropriate device packages are installed correctly on the server.
SWIM1088	Runtime error occurred while creating the device upgrade data.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1091	Minimum BootROM version of the selected image is not available in the software repository, or on Cisco.com.	The minimum BootROM value is not updated in View/Edit Image attributes for the selected image in software repository.	Update the minimum BootROM value using View/Edit Image attributes of the selected image in the software repository.
SWIM1092	Selected image does not have the minimum system software version required for system upgrade.	None.	Select an image that has a higher version than the minimum supported version. See the documentation for the Compatibility Matrix for Cisco IOS software.
SWIM1093	Cannot get Chassis Information from the inventory.	Check whether the Inventory data exists for the device in the Inventory Detailed Device Report.	If there is no inventory data for the device, schedule an Inventory Collection job and retry the task.
SWIM1094	SNMP-V3 parameters not in the Device and Credential Repository.	This could have been caused by any of the following: • The SNMP-V3 password is wrongly configured • The SNMP-V3 algorithm is wrongly configured • The SNMP-V3 engine ID is not configured in the Device and Credential Repository.	Check whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is configured in the Device and Credential Repository.
SWIM1095	Error while checking the SNMP-V3 user name in the device context.	The SNMP-V3 credentials in the Device and Credential Repository is not up to date.	Update the SNMP-V3 credentials in the Device and Credential Repository and retry the task.
SWIM1096	Selected image is not applicable to this module.	The selected image is not applicable to this module.	Use the Cisco.com Upgrade Analysis feature to find an appropriate image.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1097	Selected Bootloader image is a lower version than the version of the Bootloader running on the device.	The Bootloader image version running on the device is the latest.	Check whether the higher version is available for upgrading.
SWIM1098	The selected image is lower than the running image on the device.	The image version running on the device is the latest.	Select a higher image for device software upgrade.
SWIM1099	Image Upgrade procedure may revert to the SSH/Telnet-based approach, based on the MIB instrumentation on the running image.	The SSH/Telnet passwords may not be configured in the Device and Credential Repository.	Make sure that appropriate SSH/Telnet passwords are configured in the Device and Credential Repository.
SWIM1100	Cannot find SNMP-V2 Read-Write Community String in the Device and Credential Repository.	The SNMP-V2 credentials may not be correctly configured in the Device and Credential Repository.	Check whether the SNMP-V2 credentials are configured correctly in the Device and Credential Repository.
SWIM1101	This Device Upgrade requires opening an SSH/Telnet connection to the device.	Enable password for the device is not configured in Device and Credential Repository.	Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.
SWIM1102	This Device Upgrade requires opening a SSH/Telnet connection to the device.	There was an error while checking the credentials of the device.	Make sure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.
SWIM1103	Selected image may not be compatible to the device.	Image belongs to the same device family as the running image on the device. However, it is identified as non-compatible.	Check the Cisco.com documentation whether any caveats are identified for the selected image.
SWIM1104	The total space on the selected partition is not enough to upgrade all of the selected modules.	Multiple modules may be selected for upgrading on the same partition.	Select individual partitions for the selected modules, or deselect some modules.
SWIM1105	Image status for the selected image cannot be determined.	The selected image might be in the Deferred status.	Ensure that the image is not in the Deferred status. See the relevant documentation on Cisco.com before upgrading the images.
SWIM1106	Image selected for upgrade is compressed in .tar format. Flash will be overwritten while upgrading the image.	None.	Ensure that necessary backup jobs are completed before upgrading.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1107	This option requires *devicename* data in the inventory.	The required device information is not available in the inventory.	Perform Update Inventory and check whether the required data appears in the Detailed Device Report. If so, retry the job. Else the data is not retrieved from the device.
SWIM1109	Image status for the selected image is either Deferred or Not Supported.	Image status for the selected image is either Deferred or Not Supported.	Ensure that the image is supported by Software Management application. Check the documentation on Cisco.com before upgrading the image.
SWIM1110	.bin images are not supported for Stack Upgrade.	The .bin image has been selected for Stack Upgrade.	Select a tar image for Stack Upgrade.
SWIM1111	The available free space is not enough for upgrading this type of image.	Insufficient space for image upgrade.	Select a different image or free up some space. Update the inventory and retry the job.
SWIM1112	This module can be upgraded if managed independently.	This module can be upgraded only if it is managed as a separate device.	Assign an independent IP Address to this module. Manage it as a separate device and select that device to upgrade this module.
SWIM1113	Device Reboot failed or Reboot Verification failed.	The device is not running the new image after it is rebooted.	Verify the configuration used to load the new image. Verify whether the new image exists on the device in a valid Flash partition.
SWIM1114	The device cannot be reached after the reboot. Number of attempts to verify the device status has exceeded the maximum retry count.	Either: • An invalid image has been loaded onto the device Or • There are network connectivity problems.	Use the device console to determine if the device has reloaded with the desired image.
SWIM1115	Device is booted from TFTP server.	The backup running image is not supported.	None.
SWIM1116	Read-Write SNMP community string cannot be fetched from the Device Context.	The Read-Write community string is not available in the Device and Credential Repository for this device.	Add the Read-Write community string to the Device and Credential Repository.
SWIM1117	The selected image is incompatible and cannot run on the selected device.	The selected image is incompatible and cannot run on the selected device.	Use the Cisco.com Upgrade Analysis feature to find an appropriate image.
SWIM1118	Selected image has a lower version than the version of the running image.	The selected image has a lower version than the version of the running image.	Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1119	Telnet credentials are not present for this device. There was an error while checking the credentials of the device.	The SSH/Telnet passwords are not configured correctly in the Device and Credential Repository.	Ensure that appropriate SSH/Telnet passwords are configured correctly in the Device and Credential Repository.
SWIM1120	Cannot obtain the sysObjectID of the device.	Either: • The device did not respond when you added it to RME Or • The device cannot be added correctly.	Manually enter the device type information in the Device and Credential Repository.
SWIM1122	Runtime error found during verification.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`
SWIM1123	Telnet username not present for this device.	Either: • The Primary Credentials is not configured Or • It not configured properly for the selected device in the Device and Credential Repository.	Check whether the primary username is configured for the selected device, in Device and Credential Repository.
SWIM1124	Cannot copy the image from Flash with return code of *Code*.	None.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1125	Cannot copy the image from Flash with return code of *Code*.	None.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1126	Image copy to module failed with return code of *Code*.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC) The debug logs are available at this location: On Windows: *NMSROOT*`\files\rme\jobs\swim\`*JobID* On Solaris: `/var/adm/CSCOpx/files/rme/jobs/swim/`*Job ID*
SWIM1127	Cannot connect to device through SSH/Telnet because of *Device*.	The SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.	Check whether the SSH/Telnet credentials are correctly configured in the Device and Credential Repository.
SWIM1128	Cannot disconnect from device because of *Device*.	the SSH/Telnet credentials may not be correctly configured in the Device and Credential Repository.	Check whether the device is configured correctly.
SWIM1139	Select any available boot flash partition, for bootldr upgrade. We recommend that you use boot flash for bootldr upgrade.	This happens when the user has selected a Bootloader image for Distribution and a storage location other than bootflash.	Select any available boot flash partition for bootldr upgrade.
SWIM1150	Could not get Command Service instance for device *DeviceName* because of CmdSvc Exception.	Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.	Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.
SWIM1151	Could not connect to the device *DeviceName* because of CmdSvcException.	Either: • The device login credentials in DCR are wrong or empty. Or • The SSH option is selected in the Swim Admin pane and the target device does not support SSH.	Check whether the Login credentials in DCR and Login credentials specified during job scheduling are correct.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1161	RXBOOT credentials are not configured for the device. If TACACS is used by the device, configure RXBOOT Mode credentials in the credentials repository. This will be used to contact the device in RXBOOT Mode (if configured) for Run From Flash (RFF) devices.	RXBOOT credentials are not configured for the device in Device Credentials Repository (DCR). This will be used for Run From Flash (RFF) devices when connecting in RX boot mode.	If TACACS is used by the device, configure RXBOOT Mode credentials in the Device credentials repository.
SWIM1162	Error when recommending image for the device.	Swim recommends the image based on device ROM, RAM and Flash which it collects from RME Inventory module. If the device is having a faulty hardware (FLASH) then this will not be available in inventory.	Check the Inventory Detailed Device Report to ensure that Inventory data exists for the device (like Flash Partition size). If not, check the device for a faulty hardware or a bug in device software.
SWIM1163	Image Import from Device failed because of some unexpected error.	None.	Please contact Cisco TAC with the Job logs available under: Windows: *NMSROOT*`\CSCOpx\files\rme\jobs\swim\`*JobID* Solaris: `/var/adm/CSCOpx/files/rme/jobs/swim/`*Job ID*
SWIM1164	Image Distribute to Device failed because of some unexpected error.	None.	Please contact Cisco TAC with the Job logs available under: Windows: *NMSROOT*`\CSCOpx\files\rme\jobs\swim\`*JobID* Solaris: `/var/adm/CSCOpx/files/rme/jobs/swim/`*Job ID*

Message-ID	Error Message	Probable Cause	Possible Action
SWIM129	Selected image does not fit on the free Flash size on the device. Selected storage partition will be erased during the distribution.	Either: The boot loader image is selected for upgrade (and no system software image is selected along with it) or The storage location is not erased for the boot loader image to be copied.	Since the system software is not selected for upgrade, ensure that running system software is not in the selected storage partition. Back up the running system software and ensure that the device boots from the backed up image in case the job fails.
SWIM1501	Supervisor cannot be downgraded to an image version less than 4.1(1).	This happens when you try to distribute a CATOS image lesser than 4.1(1).	If you continue to downgrade, the device may lose its configuration. Use a higher version.
SWIM1506	Cannot move file from *Location 1* to *Location 2*.	There may not be sufficient permissions for the application to move or copy the file, or there may not be enough disk space.	None.
SWIM1507	Cannot back up the running image.	Either the file name or the storage partition name specified for backup is invalid.	You can stop the job, manually back up the running image, and retry the job.
SWIM1508	Cannot copy image *Imagename* to storage partition *Partitionname* .	Either the filename or the storage destination is invalid or the device does not provide the required MIB instrumentation for copying an image.	Retry the job. If the problem persists, check the Bug Toolkit application for any known issues on the running image version.
SWIM1510	Runtime error while performing Reload on a device.	None.	Retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\files\rme\jobs\swim\`*JobID* On Solaris: `/var/adm/CSCOpx/files/rme/jobs/swim/`*Job ID*

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1518	Runtime error during configuration upload.	None.	Check the Bug Toolkit application for any known issues on the running image version. If there are no issues, retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\files\rme\jobs\swim\`*JobID* On Solaris: `/var/adm/CSCOpx/files/rme/jobs/swim/`*JobID*
SWIM1525	Unknown package type.	None.	Check whether the module is supported in the Software Management Function and Device Support Matrix on Cisco.com.
SWIM1529	There is no module information available in the inventory for *devicename*.	There is no module information available in the inventory for *devicename*.	Update the inventory and retry the task.
SWIM1530	Storage not applicable for the Module *modulename*.	This Module does not support storage.	None.
SWIM1532	No read-write partition exists on the device to accommodate the selected image.	None	Create some free space.
SWIM1542	Minimum supported version for Supervisor is 3.8.	None.	Select a higher version of the image to upgrade.
SWIM1543	Selected image has the same or a lower version than the version of the running image.	The selected image has the same or a lower version than the version of the running image.	Verify whether the correct image is running on the device. If so, no action is required. If not, select a different image.
SWIM1546	The NVRAM size on the device may not be large enough to run the image.	The NVRAM size on the device may not be large enough to run the image.	Select a different image or upgrade the NVRAM on the device and retry the Upgrade option.
SWIM1547	Available NVRAM size on the selected image cannot be determined.	RAM size on this module may not be large enough to store this image.	Make sure the module has enough NVRAM to run the selected image. Else, select a different image or upgrade the RAM on the module.
SWIM1548	There are no software requirements found for the selected image.	None.	Select a different image.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1549	Verify that the new software selected is compatible.	Software Management cannot determine the features in the ATM software.	Check the Release Notes for the new software to determine if all the features in the old software are available in the new software.
SWIM1554	The selected image cannot be used to upgrade the device.	The device does not have any module that can run the selected image.	Select a different image.
SWIM1556	Select the Storage partition.	None.	None.
SWIM1560	Slot number corresponding to the module cannot be got from inventory.	None.	Update Inventory and retry the task.
SWIM2001	Telnet error while connecting to the device. Cannot connect to device %s.	Invalid access information in the inventory.	Verify the username and the passwords in Device and Credential Repository and retry the task.
SWIM2002	Cannot get details about Flash File system on the device.	Either the Flash device is not available or the Flash information format has changed.	None.
SWIM2503	Different images have been selected for upgrade of the Active and Stand-by processors. This may make the device unavailable.	None.	Select the same image for upgrade of Active and Stand-by CPUs.
SWIM3501	Cannot fetch device credentials for the selected device.	The credentials may not be configured correctly in Device and Credential Repository.	Check whether there are credentials are configured correctly in Device and Credential Repository.
SWIM3502	Cannot fetch the credentials of the parent device, for the selected device.	The NAM device Supervisor is not recognized by the RME Inventory.	Add the Supervisor of the NAM device to the RME Inventory.
SWIM3503	Telnet credentials are not present for the parent device.	The Telnet credentials are not properly configured for the parent device.	Check whether the Telnet credentials are configured for the parent device.
SWIM3504	If Auto Logout is enabled on the parent device, it may get disconnected during upgrade. Configure No Auto Logout for the parent device.	None.	None.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM3505	NAM images are large.	The disk space available is insufficient.	Ensure that there is enough disk space available in the htdocs/swimtemp directory under the CiscoWorks install directory.
SWIM3703	Selected image does not have the minimum system software version required for system upgrade.	None.	Select a different Image with a version higher than 11.3(0).
SWIM3705	This NRP2 is in ROMMON state. Cannot perform software upgrade on this device.	The NRP2 device is not in normal mode.	Manually bring the device into the normal mode and retry the task.
SWIM5001	Cannot connect to the device *devicename* using protocol.	The device may not be reachable or there is invalid access information in the Device and Credential Repository.	Verify whether the device is reachable and the credentials in Device and Credential Repository are correct and retry the job.
SWIM2002	Cannot get details about Flash File system on the device.	Either the Flash device is not available or the Flash information format has changed.	Done.
SWIM4602	Only image versions 6.2 or above are supported through AUS.	The image version in the device is less than 6.2.	Manually upgrade the device to a version higher than 6.2.
SWIM4800	The version running on the device is less than the minimum supported version.	None.	Manually upgrade the device to the minimum supported version or higher.
SWIM5003	Cannot copy the image.	Either the server address is incorrect or the image is inaccessible to the device.	Check whether the server address is correct and whether the image is accessible to the device.
SWIM5004	Cannot initiate SNMPset option.	The SNMP Write Community String might be wrong.	Check whether the correct SNMP Write Community String is entered in Device and Credential Repository.
SWIM5005	Device reboot option failed.	The device is not configured for reboot. The command, **`snmp-server system-shutdown`**, should be in the running configuration on the device.	Modify the device configuration and retry the job. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: On Windows: *NMSROOT*`\log\swim_debug.log` On Solaris: `/var/adm/CSCOpx/log/swim_debug.log`

Message-ID	Error Message	Probable Cause	Possible Action
SWIM5006	Device reboot option failed.	The device is not configured for reboot. The SNMP Write Community string might be wrong.	The command SNMP server system shutdown should be in the running configuration on the device. Modify the device configuration and check whether the Write Community string is configured on the device is same as the one that is entered in Device and Credential Repository.
SWIM5007	CPU switchover failed.	Either the SNMP set failed or the device is not in hot standby mode or the two CPUs are not running similar images.	Do any of the following: • Check the SNMP credentials in the Device and Credential Repository • Ensure that the device is in hot standby mode, • Ensure that the two CPUs are running similar images, before attempting the switchover.
SWIM5008	Device not responding after running the switch cpu command.	—	Check the Bug Toolkit application for any known issues on the running image version.
SWIM5009	Device is not in HotStandby Mode. Switch Operation terminated.	The Standby CPU may be down.	Bring up the standby CPU and retry the job.

Syslog Analyzer and Collector

This section provides the troubleshooting information and FAQs for the Analyzer and Collector application:

- Syslog Analyzer and Collector FAQs
- Troubleshooting Syslog Analyzer and Collector

Syslog Analyzer and Collector FAQs

- Q.Why am I not getting syslog messages for my devices?
- Q.Where does RME keep Syslog messages?
- Q.When I tried to generate a syslog report I got an outofmemory exception. Why does this happen?
- Q.Where can I get the description of the error messages?
- Q.How do I change the location of the syslog.log file??
- Q.How do I check the size of the syslog.log file, and delete it when required?

Q. Why am I not getting syslog messages for my devices?

A. You might not be getting syslog messages for one of the following reasons:

- The device is not managed by RME.
- The Syslog parameters are not enabled correctly on the device.

- Too many messages are being received by the syslog program. On Windows systems, logging for the PIX firewall has a tendency to lock the syslog function due to the massive number of messages from the firewall.
- Filters might be applied to incoming syslog messages. By default, Link Up/Down, PIX, Severity 7, and IOS Firewall Audit Trail messages are filtered out.

Q. Where does RME keep Syslog messages?

A. For the location of the log file (syslog.log) that contains syslog information, check the SYSLOG_FILES property in the Collector.properties file.

This file is available at the following location: *NMSROOT*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data, where *NMSROOT* is the CiscoWorks install directory.

Q. When I tried to generate a syslog report I got an outofmemory exception. Why does this happen?

A. When you are generating a syslog report, you may sometimes get an outofmemory exception.

This may occur if the number of syslog messages that were generated in the Date Range that you specified for the syslog report job, exceed 0.6 million.

Specify a shorter Date Range in the Report Generator (**Resource Manager Essentials > Reports > Report Generator**), and run the report job again.

Q. Where can I get the description of the error messages?

A. To get the description of the error messages follow either of these procedures:

Procedure 1

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Report Generator dialog box appears, in the Report Generator page.

Step 2 From the first drop-down list box, select Syslog.

Step 3 From the second drop-down list box, select the Standard Report.

Step 4 Select the required devices using the Device Selector.

For details about the Device Selector, see the topic Using RME Device Selector in Chapter 3: Adding and Troubleshooting Devices Using Device Management of the *User Guide for Resource Manager Essentials 4.1*.

Enter the date range and select the Run Type as **Immediate**.

Step 5 Click **Finish**.

The Standard Report appears.

Step 6 Click on * in the details column for the respective device name.

Procedure 2

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The RME Report Generator dialog box appears, in the Report Generator page.

Step 2 From the first drop-down list box, select Syslog.

Step 3 From the second drop-down list box, select the **Unexpected Device Repor**t.

Step 4 Select the required devices using the Device Selector.

For details about the Device Selector, see the topic Using RME Device Selector in Chapter 3: Adding and Troubleshooting Devices Using Device Management of the *User Guide for Resource Manager Essentials 4.1*.

Step 5 Enter the date range and select the Run Type as **Immediate**.

Step 6 Click **Finish**.

The Unexpected Device Report appears.

Step 7 Click on * in the details column for the respective device name.

Q. How do I change the location of the syslog.log file?

A. The file from which syslog messages are read, is syslog.log. The default location of the file is:

On Solaris:

/var/log/syslog_info

On Windows:

%NMSROOT%\log\syslog.log

However, you can change the location of this file. To change the location of the syslog.log file, you should appropriately modify the Syslog Collector Properties file (filename: Collector.properties) which is available at:

- On Solaris: *$NMSROOT*/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties
- On Windows: *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties

The following procedure shows you how the location of the syslog.log file can be changed on Solaris and Windows:

On Solaris

Step 1 In the syslog configuration file, syslog.conf, (available at /etc/syslog.conf) look for local7 and change the location of the syslog.log file.

A new file, syslog.log, will be created in this location. Make sure that this new file has read permissions to casuser.

Step 2 Ensure that the syslog process (syslogd) can both read and write to the file.

Step 3 Restart the syslog process (syslogd). Enter the following commands to stop and restart syslogd:

```
/etc/init.d/syslog stop

/etc/init.d/syslog start
```

Step 4 Stop the SyslogCollector process. To do this:

a. Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

b. Select **SyslogCollector** and click **Stop**.

Step 5 Edit the SYSLOG_FILES property in the Collector.properties file to reflect the changed location.

The Collector.properties file is located at: *$NMSROOT*/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties

Step 6 Start the SyslogCollector process. To do this:

a. Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

b. Select **Syslog Collector** and click **Start**.

Step 7 Update the location of the syslog.log file in the logstat.conf file.

The logstat.conf file is located at /opt/CSCOpx/conf.) This ensures that the new syslog.log file is referenced when you generate a Log File Status report (**Common Services > Server > Reports > Log File Status**.

On Windows

Step 1 Edit the location of the syslog.log file in the LogFile (available at *HKEY_LOCAL_MACHINE\SYSTEM*\CurrentControlSet\Services\crmlog\Parameters\) in Registry Editor (REGEDIT).

A new file, syslog.log, will be created in this location. Make sure that this new file has read permissions to casuser.

Step 2 Stop and restart CWCS syslog service. To do this:

a. Go to Services (**Start > Programs > Administrative tools > Services**).

b. Select CWCS syslog service, and click **Stop**.

c. To restart the syslog service in the Control Panel, click **Start** next to the CWCS syslog service.

Step 3 3) Stop the SyslogCollector process. To do this:

a. Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

b. Select SyslogCollector and click **Stop**.

Step 4 Edit the SYSLOG_FILES property in the Collector.properties file to reflect the changed location.

The Collector.properties file is located at: *%NMSROOT%*\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties.

Step 5 Start the SyslogCollector process. To do this:

a. Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

b. Select SyslogCollector and click **Start**.

Step 6 Update the location of the syslog.log file in the logstat.conf file.

The logstat.conf file is located at *NMSROOT*\CSCOpx\conf.) This ensures that the new syslog.log file is referenced when you generate a Log File Status report (**Common Services > Server > Reports > Log File Status**.

Q. How do I check the size of the syslog.log file, and delete it when required?

A. You can check the size of the syslog.log file by generating the Log File Status report. To do this:

Step 1 Go to **Common Services > Server > Reports > Log File Status.**

The Reports Generator dialog box appears.

Step 2 Click **Log File Status** and then click **Generate**.

The Log File Status report appears.

If the File Size is displayed in red it means that the file has exceeded its size limit. If the File System Utilization is displayed in red it means that the file exceeds 90% utilization.

You should reduce the size of your log file if your file system utilization is over 90%. You can:

c. Back up the log file.

To back up your log files, see Maintaining Log Files in Chapter 4: Configuring the Server in the *User Guide for CiscoWorks Common Services* by accessing the following link:

http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html

d. Stop the Syslog Analyzer (**Start > Settings > Control Panel > Services**).

For the procedure, see "Deleting the Log File".

e. Delete the file.

For the procedure, see "Deleting the Log File".

Deleting the Log File

To delete the log file:

Note View the Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Common Services > Server > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select **SyslogAnalyzer** and click **Stop**.

Step 3 Open the Windows Control Panel and select **Administrative tools > Services**.

Step 4 Select **CWCS syslog service**, and click **Stop**.

Step 5 Delete the log file in:

- *NMSROOT*\log\syslog.log file on Windows.

  or

- /var/log/syslog_info on Solaris.

Step 6 Restart the CWCS syslog service and the SyslogAnalyzer process:

- To restart the syslog service in the Control Panel, click **Start** next to the **CWCS syslog service**.
- To restart the SyslogAnalyzer process in RME, select **Common Services > Server > Admin > Processes** and click **Start**.

Troubleshooting Syslog Analyzer and Collector

This section provides the troubleshooting information for the Syslog Analyzer and Collector application:

Message ID	Error Message	Probable Cause	Possible Action
SLCA0114	{0}[1] could not be exported.	Either file specified already exists or file specified does not have permissions to write.	• Choose another file or allow overwrite by checking overwrite file option. • Give write permissions to the selected file or choose another file with the valid permission. The casuser must have the write permission.
SLCA0115	{0}[1] could not be imported.	None.	Check if file {1} [2]specified exists, has read permissions and contains valid {0}[1] Check if the database is running normally.
SLCA0122	Cannot schedule job in the past, Current Server {0}[3], please enter proper schedule.	You have scheduled a job in the past.	Select a future date.
SLCA0126	Could not subscribe to the Collector.	None.	• Check if the collector is running. • Make sure that SSL certificates are imported/exported correctly and process restarted. • Check if the Certificates exported/imported are valid and have not expired. • Check if SyslogAnalyzer process is running.

Message ID	Error Message	Probable Cause	Possible Action
SLCA0130	{0}[4] location does not have permissions to create files for backing up data.	None.	Give write permissions or change the location and try again.
SLCA0131	There are more than {0}[5] records generated for this date range. Only {0}[5]. records are being displayed, starting with the records generated on the end date.	None.	To view the complete report, schedule a job that does not have Immediate as the Run Type.

1. Displays the task name, Automater Action or Message Filter
2. Displays the filename.
3. Displays the current date and time
4. Displays the location
5. Displays total number of records

Job Approval

This section provides the troubleshooting information for the Job Approval application:

Message ID	Error Message	Probable Cause	Possible Action
JBAP0001	Cannot enable approval for applications that do not have an Approver-List assigned to them	You have attempted to enable Approval without assigning a list to the application.	Go to the **Approval** > **AssignLists** screen and assign a list to the application. Enable Approval again.
JBAP0002	Specify a valid E-mail address.	You have entered an invalid E-mail-address.	Enter a valid E-mail address
JBAP0003	Select at least one job.	You have attempted to perform an action on a job without selecting a job	Select a job before performing an action on it.
JBAP0004	Select only one job.	You have attempted to view JobDetails, with more than one job selected	Select only one job.
JBAP0005	List {0} has no users. To save the list successfully, add users and click **Save**	This is not an error. This is an Information message when you adda list for the first time.	Add users before saving the list
JBAP0006	{0} is not a valid Approver. Enter a user with Approver role	You have attempted to add a user who has not been added as Approver in CMF.	You must first add the user as Approver into CMF. Only then can you add this user into RME.
JBAP0007	Select an Approver, to change E-mail.	You are trying to do a 'Save' without selecting a user.	Go back and select a user.

Message ID	Error Message	Probable Cause	Possible Action
JBAP0008	List {0} already exists.	You have attempted to add a list that already exists.	Add the list with a different list name.
JBAP0009	Could not approve/reject the job {0}. Verify that the database and mail server are running.	Either approve/reject mails cannot be sent, or the database is not running.	Make sure mail server is configured properly and that the database is running.
JBAP0010	Cannot reject a job without comments.	You have attempted to reject a job without giving reasons for rejecting	Add comments if you want the job to be rejected.
JBAP0011	Select a future start date.	You have selected a past date while changing a job schedule	Select a future date.
JBAP0012	Job {0} is changed successfully.	Not an error message	None.
JBAP0013	Are you sure you wish to delete? Approval will be disabled for applications to which {list-name} is assigned.	Alert message before deleting – not an error message.	None.
JBAP0014	Enter a valid Approver-List name.	You may have entered invalid characters such as spaces in the Approver name.	Add a valid user-name
JBAP0015	{list-name} already exists.	You have attempted to add a list name that already exist	Select a different name
JBAP0016	{user-name} already exists.	You have attempted to add a user name that already exists.	Add a new user name. This field is case-sensitive.
JBAP0017	Are you sure you wish to delete? This will disable approval for applications having {user-name} as the sole approver.	Warning message for deleting a user. If you have enabled Approval for an application whose sole approver is this user, it will be disabled.	None.
JBAP0018	You have attempted an action without selecting a user. Select a user before performing the action.	User not selected.	Select a user before performing the action.
JBAP0019	You have attempted an action without selecting a list. Select a list before performing the action	List not selected.	Select a list before performing the action

Message ID	Error Message	Probable Cause	Possible Action
JBAP0021	Cannot save a list that has no approvers in it.	No approver available for the selected list.	Add approvers before trying to save the list.
JBAP0022	Cannot change schedule for {0}. A runtime error occurred when you tried to change the schedule of the job. See the Troubleshooting section of the RME 4.1 help.	None.	This exception will appear in the MakerChecker.log in the following location: *NMSROOT*`\log` where *NMSROOT* is the CiscoWorks install directory. Contact Cisco Technical Assistance Center (TAC) with this log file.
JBAP0024	Cannot send approval E-mails. Make sure that SMTP Server is configured correctly.	None.	Go to **Common Services > Server > Admin > System Preferences** and configure SMTP Server correctly.

Bug Toolkit

This section provides the troubleshooting information for the Bug Toolkit application:

Troubleshooting Bug Toolkit

Message ID	Error Message	Probable Cause	Possible Action
BTKT0001	Report data not found.	Bugs may not be available for the selected device(s).	None.
BTKT0002	Report name not found.	None.	None.
BTKT0003	You have not selected any device.	No device selected.	Select at least one device.
BTKT0004	You have selected an invalid date.	The date is invalid. It may be a past date.	Select a future date
BTKT0005	Error while formatting the selected date.	The date may be invalid. -	Check if the selected date is valid
BTKT0006	Job creation failed.	None.	Check bugtoolkit.log for more details.
BTKT0007	No Bug ID found.	You have not entered a Bug ID.	Enter a Bug ID or a group of Bug IDs separated by commas.
BTKT0008	Invalid Bug ID found in the input: {0	You have entered an invalid Bug ID.	Enter a valid Bug ID
BTKT0009	No data found in the input file	None.	None.
BTKT0010	No details found in Cisco.com for the given bugs input.	There is no information in Cisco.com for this bug.	None.

Message ID	Error Message	Probable Cause	Possible Action
BTKT0011	The Cisco.com interface did not return any information for all the bugs.	Information is not available for the bugs that you have entered. The bugs may be invalid or you may not have privilege to access them.	Check whether the bugs are valid and also whether you have permission to see them.
BTKT0012	Input file not found.	The input file name is invalid.	Select a valid input file.
BTKT0013	Information could not be fetched from Cisco.com. Please check User Guide for RME for more details.	Information could not be fetched from Cisco.com either because information not available on Cisco.com or the system could not connect to Cisco.com.	Check if the Cisco.com credentials are correct. If credentials are correct, check the proxy server configuration if direct connection to Cisco.com is unavailable from CiscoWorks Server. You can check the proxy server configuration using Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup.
BTKT0014	Information could not be fetched from Cisco.com. Please check User Guide for RME for more details.	Information could not be fetched from Cisco.com either because information not available on Cisco.com or the system could not connect to Cisco.com.	Check if the Cisco.com credentials are correct. If credentials are correct, check the proxy server configuration if direct connection to Cisco.com is unavailable from CiscoWorks Server. You can check the proxy server configuration using Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup.
BTKT0015	Inventory data does not exist for the device(s) selected. So could not find the report.	The devices that you have selected for this report do not have any Inventory data.	Ensure that the Inventory data is collected for these devices.
BTKT0016	Problem with posting and getting the results from Cisco.com	The Cisco.com Server may be down.	Try again later.
BTKT0017	Enter Job Description	There is no Job Description.	Enter Job Description.
BTKT0018	Enter a valid E-mail address	You have entered an invalid E-mail address.	Enter valid E-mail address
BTKT0019	Internal error: Cannot schedule a job.	Either the CTMJrmServer or the JrmServer may not be running	1. Check the status of JRMServer using the pdshow command 2. Start JRM and try creating the job.

Message ID	Error Message	Probable Cause	Possible Action
BTKT0020	Device(s) are not supported by Cisco.com.	For a device to get the details of its bug from the Cisco.com database, the device must have been added to this database. In this case it has not been added.	Check bugtoolkit.log for more details.
BTKT0021	Cannot retrieve the URL limits or the Thread limits.	• Either: The Bugtool.properties file does not exist Or • The Bugtool.properties file exists but with wrong url and thread limits or no url or thread limits.	Check whether the file Bugtool.properties exists or if you have entered the values correctly or ensure that the url limits and thread limits are given in the Bugtool.properties file and the file exists.
BTKT0022	Devices are not supported by Cisco.com or Cisco.com URL	Connection Timeout.	Try again later.

cwcli config

This section provides the troubleshooting information for the cwcli config commands:

Message-ID	Error Message	Probable Cause	Possible Action
CCLI0001	Could not get any device(s) to work on.	This problem occured because of any of the following: • Specified device(s) is not managed by RME. • You have not used the correct Device Display name • DCR server is down	Do any of the following, depending on what caused the problem: • Specify valid devices that are managed by RME • Use a valid Device Display name. • Use the pdshow command to verify whether the DCR server is running.
CCLI0002	The job could not be created since no device is available.	This problem occured because of any of the following: • You have entered invalid arguments for the command. • You have entered devices that are not managed by RME. • CTMJrmServer and jrm are down. • ConfigMgmtServer process is down.	Do any of the following, depending on what caused the problem: • Enter valid arguments. • Verify that the devices you have entered are managed by RME. • Use the pdshow command to verify whether the CTMJrm server and jrm are running. • The ConfigMgmtServer process should be up for the configuration Download and Fetch options.

Message-ID	Error Message	Probable Cause	Possible Action
CCLI0003	Could not get results for devices within the specified time interval	Less timeout is configured	Either: • Increase the timeout value using the **-timeout** option. Or • Use Archive Management's Job Browser to see the results.
CCLI0004	Could not retrieve the Device Identification number for the device.	This problem occured because of any of the following: • Specified device(s) is not managed by RME. • You have not used the correct Device Display name • DCR server is down	Do any of the following, depending on what caused the problem: • Specify valid devices that are managed by RME. • Use a valid Device Display name. • Use the pdshow command to verify whether the DCR server is running.
CCLI0005	There are no archived configurations for this device	Sync Archive has not happened for the specified device.	Archive the configuration using the Sync Archive feature. For details on using the Synch Archive feature, see the Online Help.
CCLI0006	Cannot create a temporary file to store the running configuration.	This problem occured because of any of the following: • There is not enough space to create a file in your file system. • You do not have permissions to create a file in the specified location.	Do any of the following, depending on what caused the problem: • Verify whether there is enough space to create a file in your file system. • Verify whether you have permissions to create a file in the specified location.
CCLI0007	Cannot retrieve the configuration file from the archive.	The specified version does not exist in the archive.	Verify whether the specified version exists in the archive. Use the **listversions** command to see the available versions.
CCLI0008	Could not create a temporary file in DCMA temporary directory.	This problem occured because of any of the following: • There is not enough space to create a file in your file system. • You do not have permissions to create a file in the specified location.	Do either of the following, depending on what caused the problem: • Verify whether there is enough space to create a file in your file system. • Verify whether you have permissions to create a file in the specified location.
CCLI0009	Cannot get running configuration.	The archive does not contain any versions for the device.	Verify whether the specified version exists in the archive. Use the **listversions** command to see the available versions.
CCLI0010	Device has only one version archived.	Synch Archive has not happened for the specified device	Archive the configuration using the Synch Archive feature. For details on using the Synch Archive feature, see the Online Help.

Message-ID	Error Message	Probable Cause	Possible Action
CCLI0011	The specified version of the configuration does not exist.	You have entered an invalid version of the configuration.	Use the **listversions** command to see the available versions and enter an existing version
CCLI0012	No baseline templates exist for this device.	None.	Use the **listversions** command to see the available baseline templates.
CCLI0013	Data file does not contain any device.	None	Add the devices in the data file and try again
CCLI0014	The job could not be created because of the errors reported.	This problem occured because of any of the following: • You have entered invalid arguments. • The data file is missing some parameters.	Do either of the following, depending on what caused the problem: • Verify whether you have entered valid arguments. • Update the data file if there are missing parameters.
CCLI0015	You should not use the **-f** option with more than one device.	Multiple devices are specified for the command to be executed along with **-f** option	Use the **-input** option to specify the file for every device

cwcli export

This section provides the FAQs for the `cwcli export` tool:

- Q.What does cwcli export do?
- Q.What is ComputerSystemPackage Class?
- Q.Where does `cwcli export` collect the configuration information from?
- Q.Is the containment hierarchy in inventory schema exactly the same as that in CIM?
- Q.What is an XSD file?
- Q.What is the AdditionalInformation tag in the inventory schema used for?
- Q.How do I know what fields come under AdditionalInformation?
- Q.Where can I find information specific to a particular node which I can see in detailed device information but not in `cwcli export`.?
- Q.How can I make use of the servlet interface?
- Q.How can I get data for some particular entity from devices which are managed by different RME servers?
- Q.While using the -m option, can I use more than one E-mail id?
- Q.Where can I get the descriptions of each node in the schema?
- Q.Why am I getting parse error when trying to parse some of the output files?

Q. What does cwcli export do?

A. **`cwcli export`** is a command line tool that also provides servlet access to export inventory, configuration and change audit data. You can use this tool to export inventory, configuration archive, and change audit data for devices in Resource Manager Essentials (RME), in the XML format.

The Data Extracting Engine (DEE) of RME 3.5, is now part of the CWCLI framework. You can use the **`cwcli export`** command to generate the Inventory and Configuration data in XML format. In addition to this, you can also export Change Audit data.

See these topics in the RME Help:

- *Running cwcli export changeaudit* for the usage and XML schema details.
- *Running cwcli export config* for the usage and XML schema details.
- *Running cwcli export inventory Command* for the usage and XML schema details.

Q. What is ComputerSystemPackage Class?

A. It is the class that contains the InstanceIDs of Cisco-Chassis and Cisco-NetworkElement, and relates the two.

Q. Where does **`cwcli export`** collect the configuration information from?

A. **`cwcli export`** collects the running configuration data from the latest configuration in the Config Archive.

Q. Is the containment hierarchy in inventory schema exactly the same as that in CIM?

A. No. Although the containment hierarchy in inventory schema is based on Common Information Model (CIM), it does not follow the exact containment hierarchy because of the limitations in the RME database schema.

Q. What is an XSD file?

A. XSD file is an XML based alternative to Document Type Definition (DTD). It is based on XML schema language which describes the structure of an XML document. An XML schema defines the legal building blocks of an XML document, just like a DTD.

An XML Schema:

- Defines elements that can appear in a document.
- Defines attributes that can appear in a document.
- Defines which elements are child elements.
- Defines the order of child elements.
- Defines the number of child elements.
- Defines whether an element is empty or can include text.
- Defines data types for elements and attributes.
- Defines default and fixed values for elements and attributes.

Q. What is the AdditionalInformation tag in the inventory schema used for?

A. The AdditionalInformation tag is provided to define information that is specific to a device. The inventory schema may not contain information for all the elements in all the devices supported by **`cwcli export.`** The AdditionalInformation tag addresses scenarios where the inventory schema does not have tags to define information that you want to collect for some of the elements in a particular device.

Q. How do I know what fields come under AdditionalInformation?

A. For this information, see the topic, Additional Information Table, in the RME Online Help.

Q. Where can I find information specific to a particular node which I can see in detailed device information but not in `cwcli export.`?

A. For this information, see the topic, Additional Information Table, in the RME Online Help.

Q. How can I make use of the servlet interface?

A. You must write customized scripts which could connect to the servlet. The arguments and options have to be specified in XML format.

For more details, see the section, Using cwcli Commands in the RME Online Help.

Q. How can I get data for some particular entity from devices which are managed by different RME servers?

A. You have to write a script to connect to different RME servers and aggregate all data into a single file. After you get the aggregated data, you can parse it and get the data for any required entity.

Q. While using the -m option, can I use more than one E-mail id?

A. No. You can use only one E-mail address at a time, when you use the `-m` option of the `cwexport` command.

Q. Where can I get the descriptions of each node in the schema?

A. You can find the descriptions in the RME Online help. See the topic Overview: cwcli export and sub-topics.

Q. Why am I getting parse error when trying to parse some of the output files?

A. Some of the classes in IDU and Optical switches contains some special characters with ASCII code larger than 160. Most of the XML parsers does not support these characters and hence fails to parse these characters.

To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:
If there is an element,
checksum `¢Úo` */checksum*
you must change it to
checksum `<![CDATA[¢Úo ]]>` */checksum*

NetShow

This section provides the FAQs and troubleshooting information for the NetShow application:

- NetShow FAQs
- Troubleshooting NetShow

NetShow FAQs

- Q.How can I add an adhoc command to only one particular device category in a command set?
- Q.How do I mask the credentials shown in NetShow job output?
- Q.Why am I not able to delete some adhoc commands?
- Q.What are the valid adhoc commands that I can enter?
- Q.Why are the system-defined command sets not displayed in the assign command sets flow?

- Q.What do I enter in the custom commands field during job creation?
- Q.Where can I specify the protocol order for NetShow?
- Q.Where can I specify the job policies for NetShow?
- Q.Why are the system-defined commands inside a command set, not shown based on device category?
- Q.How do I view the consolidated output of all the devices and the commands executed on these devices?
- Q.What is Output Archive?
- Q.When is the output of a command archived?
- Q.When I delete a job, does the corresponding archive also get deleted?
- Q.In the Output Archive page, what does Success = and Fail = under the heading Status mean?
- Q.Why do devices show Fail status in NetShow jobs?

Q. How can I add an adhoc command to only one particular device category in a command set?

A. You need to choose that particular device category while creating the command and enter the adhoc command.

Q. How do I mask the credentials shown in NetShow job output?

A. You need to update the properties file
NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm
\rmeng\config\netshow\NSCredCmds.properties file
with the command for which the credentials are displayed.

We recommend that you enter the complete command in the file. For example, you must enter **`show running-config`**, not
`show run.`

Q. Why am I not able to delete some adhoc commands?

A. You can delete adhoc commands only if they are not part of any command set. So in the Edit flow, you need to remove the command from the selected commands list and click **Finish**. Then you can edit the command set again and try deleting the adhoc command.

Q. What are the valid adhoc commands that I can enter?

A. **`show`**, **`version`**, **`where`**, **`ping`**, **`traceroute`**, and **`?`**. You can use the short forms of these commands. For example you can use **`sh`** for **`show`**.

Q. Why are the system-defined command sets not displayed in the assign command sets flow?

A. System-defined command sets are by default assigned to all. Since the system-defined command sets are already assigned to all users, they will not appear in the assign command sets flow.

Q. What do I enter in the custom commands field during job creation?

A. Enter the adhoc commands. These adhoc commands are downloaded on all devices even if a particular device does not support the command.

Q. Where can I specify the protocol order for NetShow?

A. See Defining Protocol Order, in *Chapter: 11 Using NetShow Commands* in the *User Guide for Resource Manager Essentials 4.1.*

Q. Where can I specify the job policies for NetShow?

A. See the topic, Job Options, in *Chapter: 11 Using NetShow Commands* in the *User Guide for Resource Manager Essentials 4.1*.

Q. Why are the system-defined commands inside a command set, not shown based on device category?

A. The system-defined commands do not map to a particular device category inside a command set.When you run a job, these commands will be downloaded on all applicable devices.

Q. How do I view the consolidated output of all the devices and the commands executed on these devices?

A. You can view the output of all the commands for all the devices by clicking the Print button on the top right hand corner of the NetShow Job Details page.

Q. What is Output Archive?

A. The Output Archive feature in NetShow helps you archive and access the stored output that is created from a NetShow job.

The Output Archive will not display the Job Summary and Work Order details, to view these see topic Viewing Job Details, in *Chapter: 11 Using NetShow Commands* in the *User Guide for Resource Manager Essentials 4.1*.

Q. When is the output of a command archived?

A. The command output is archived only if the job was executed completely. Cancelled jobs are not archived.

Q. When I delete a job, does the corresponding archive also get deleted?

A. No. If you want to delete an archive, you can do so from the Output Archive page.

Q. In the Output Archive page, what does **Success =** and **Fail =** under the heading **Status** mean?

A. It indicates the number of devices on which a particular command execution was successful and the number of devices on which it failed.

Q. Why do devices show **Fail** status in NetShow jobs?

A. A device will show **Fail** status if it is unreachable or if a single command execution fails.

Troubleshooting NetShow

Message ID	Error Message	Probable Cause	Possible Action
NS0001	Could not get details for command set.	RMEDbEngine may be down.	Check whether RMEDbEngine is running properly. If not, restart it and try again.
NS0002	You have not selected a device category.	You did not select a device category while creating a new Command Set.	Select a device category in the Select Device Category page.
NS0003	You have not selected any commands.	You did not select any commands.	Selected any commands in the Select Commands page.

Message ID	Error Message	Probable Cause	Possible Action
NS0004	Could not create Command Set. Check whether RMEDbEngine is running properly. If not, restart it and try again.	RMEDbEngine may be down.	Check whether RMEDbEngine is running properly. If not, restart it and try again.
NS0005	Could not edit Command Set. Check whether RMEDbEngine is running properly. If not, restart it and try again.	RMEDbEngine may be down.	Check whether RMEDbEngine is running properly. If not, restart it and try again.
NS0006	Edit option not allowed for System-defined command sets. Select a User-defined command set to edit.	You may have tried to edit System-defined command sets.	You cannot edit System-defined command sets. Select a User-defined command set to edit.
NS0007	Adhoc commands are not valid.	You may have entered invalid adhoc commands	Enter valid adhoc commands. See the Online help for the list of valid adhoc commands. Separate multiple commands with commas.
NS0008	This option is not allowed for System-defined command sets.	You may have tried to perform an invalid job for the System-defined command sets.	Select a user-defined command set and continue to create or edit jobs.
NS0009	Command Set with this name already exists.	You may have entered an existing command set name.	Enter a unique command set name and continue to create the command set.
NS0010	You have not selected any adhoc commands.	You may not have selected any adhoc commands while deleting commands.	Select the commands to be deleted and continue with deleting the command set.
NS0011	The commands are not deleted. This is because they may be system-defined or part of a command set or in the selected commands list.	You may have selected any of the following: • System-defined commands • Commands that are part of a Command Set • Commands in the selected list	Select a User-defined commands and continue. Also check whether the adhoc command is in this command set or in any other command set.
NS0012	You have not specified any adhoc commands Enter the commands to be added.	You did not specify any adhoc commands while adding adhoc commands in the new command set.	Enter valid adhoc commands to be included in the command set and click **Add Adhoc** to include the adhoc command in the new command set.
NS0013	The username is invalid or not authorized.	You may have entered an invalid or unauthorized username while assigning command sets or showing assigned command sets.	Enter a valid or authorized username and continue to assign command sets or show assigned command sets.
NS0014	You have not selected a command set.	You did not select a command set.	Select a command set in the previous screen and continue to create or edit jobs.

Message ID	Error Message	Probable Cause	Possible Action
NS0015	The username is invalid or not authorized. Command sets are not assigned to this user.	You may have selected an invalid or unauthorized user. You may also have selected a user to whom no command sets are assigned.	Select a valid or authorized user. Also, select a user to whom command sets are assigned.
NS0016	Could not stop following jobs {0}. This is because the job may have already completed. You can only stop running jobs. See the Online help for details on stopping running jobs.	This is because you may have tried to stop a job has already completed.	You can only stop certain running jobs. See the Online help for details on stopping running jobs.
NS0017	Could not delete following jobs.	These jobs may be running.	You cannot delete running jobs.
NS0018	You cannot edit this job since the scheduled time has elapsed.	You have tried to edit a job whose scheduled completion time has elapsed.	You cannot edit a job that has already completed running.
NS0019	You have not selected any devices.	You have not selected any devices.	Select any device in the Select Devices and Command Sets screen and continue to create or edit jobs.
NS0020	You have not selected any command set or entered any adhoc commands.	You did not select any command set or enter any adhoc commands.	Select a command set or enter an adhoc command in the Select Devices and Command Sets screen and continue to create the job.
NS0021	You are not authorized to run custom commands.	You do not have privileges to run custom commands.	You must get permission to run these commands.
NS0022	You have not selected any device or command sets. You also have not entered any custom commands.	You did not select any device or command sets. You also have not entered any custom commands.	Select at least one device and command set and enter custom commands.
NS0023	Job Approval is enabled. Do not select Immediate.	You may have enabled Job Approval and tried to schedule an immediate job.	Do not schedule an immediate job if you have already enabled job approval.
NS0024	You have entered a past date/time for creating the job.	You have entered a past date or time for creating a job.	Schedule this job to run either immediately or at a future date and time.
NS0025	Notification E-mail address is not valid.	You may have entered an invalid E-mail.	Enter the E-mail this format: a@b.c.
NS0026	Enter the Maker E-mail ID.	You may not have entered the Maker E-mail ID.	Enter the Maker E-mail ID.
NS0027	Maker E-mail address is not valid.	You may have entered an invalid Maker E-mail address.	Enter a valid Maker E-mail address.

Message ID	Error Message	Probable Cause	Possible Action
NS0028	Could not create job.	CTMJrmServer and JRM processes may not be running properly.	Check whether CTMJrmServer and JRM processes are running properly. If not, restart them and try again.
NS0029	Could not delete the job(s)	You may have tried to delete a running job.	Try deleting the job after the job has completed running.
NS0030	Could not stop job.	You may have tried to stop jobs that are currently completed.	You cannot stop jobs that are already completed.
NS0031	Only one job can be stopped at a time.	You may have tried to stop more than one job at a time.	Select only one job and try to stop it.
NS0032	Could not get details for job.	CTMJrmServer and JRM processes may not be running properly.	Check whether CTMJrmServer and JRM processes are running properly. If not, restart it and try again.
NS0033	Error occured while processing.	CTMJrmServer and JRM processes may not be running properly.	Check whether CTMJrmServer and JRM processes are running properly. If not, restart it and try again.
NS0034	Enter a value for the filter.	You may not have entered a value for the filter.	Select a value from the Filter by list and continue filtering the jobs.
NS0035	The device does not exist.	The device may not be managed through RME.	Add the device with proper credentials and try again.
NS0036	None of the commands have applicable commands.	You may have selected devices that do not have applicable commands.	Select commands that have applicable commands.
NS0037	Could not delete the following archives.	The archives you are trying to delete, do not exist.	Some other user must have deleted the archive. Refresh the page to make sure that the archive has been deleted.
NS0038	Running jobs cannot be deleted.	You may have tried to delete a running job.	You cannot delete a running job.
NS0039	Could not get details for the job.	CTMJrmServer and JRM processes may be down.	Check whether CTMJrmServer and JRM processes are running properly. If not, restart them and try again.
NS0040	Description cannot be more than 256 characters.	You may have tried to a enter job description that has more than 256 characters.	Enter a description with less than 256 characters.
NS0041	Retry is not supported on periodic jobs.	You may have tried to retry a periodic job.	You can retry only immediate or non-periodic jobs.
NS0042	Cisco.com user credentials are not valid. Enter correct credentials.	The Cisco.com credentials entered are invalid.	Enter correct credentials.
NS0043	The Output Interpreter tool could not analyze the output.	This may be because caused by a problem while connecting to Cisco.com or with Cisco.com, itself.	Check whether Cisco.com connection is proper and try again.

Message ID	Error Message	Probable Cause	Possible Action
NS0044	Enter the username.	You may not have entered a username while assigning command sets or showing assigned command sets.	Enter the username and continue to assign command sets or show assigned command sets.
NS0045	User is an administrator. All command sets are assigned to this user by default.	You may have tried to assign command sets to a user with Administrative privileges.	By default, all command sets are assigned to the Administrator.
NS0046	Enter job description.	You may not have entered the job description.	Enter a description for the job.
NS0047	Enter the login username.	You may not have entered the device login username.	Enter the login username and continue to schedule the job.
NS0048	You have no jobs.	There are no jobs scheduled or running.	You can create new jobs using the NetShow job browser.
NS0049	You have no archives.	There are no job archives.	You can create new jobs using the NetShow job browser. The output of these jobs will be archived.
NS0050	You can retry only failed jobs.	You may have retried running or successful jobs.	You can retry only failed jobs.
NS0051	The job has already stopped.	You may have tried to stop a job that has already stopped.	Select a job that is running or scheduled to stop.

Administration

This section provides the FAQs for the Administration module:

Admin FAQs

- Q.What is Collection Failure Notification and how is it carried out?
- Q.What does a Trap Notification message contain?
- Q.Is Notification on Failure option configurable?
- Q.How can I listen to the Trap Notifications on Inventory and/or Config Collection failure?
- Q.How can I change the default Report Archive location to Custom location?
- Q.Why does the Contract Status Detailed Report show no records for a valid contract?

Q. What is Collection Failure Notification and how is it carried out?

A. In RME, Config and Inventory collection are carried out either through manual jobs or system based collection. During this collection, the Config Collection or Inventory Collection may fail. These failure trap messages are broadcast through the default port 162, to the hosts connected to the same subnet where the Ciscoworks server is located. The port or the destination is not configurable.

Q. What does a Trap Notification message contain?

A. A Trap Notification message consists of:

- Application Name - Either Config or Inventory
- Device Display Name
- Collection Failure Time
- Reason for Failure

Q. **Is Notification on Failure option configurable?**

A. Yes. You can configure this Notification on Failure option by using the Collection Failure Notification option available under:

RME > Admin > System Preferences > Collection Failure Notification.

You can configure the broadcast of Traps on either Config collection failure or Inventory collection failure or both.

After installing RME, the broadcast of Trap notification on collection failure is enabled for both Config and Inventory by default. You can disable this option, if you do not want to track the Inventory and Config collection traps.

Q. **How can I listen to the Trap Notifications on Inventory and/or Config Collection failure?**

A. You can install a third party Trap receiving tool on any host in the subnet to receive such Trap messages.

Q. **How can I change the default Report Archive location to Custom location?**

A. To change the default Report Archive location:

Step 1 Go to **Resource Manager Essentials** > **Admin** > **Reports** > **Archive Settings**.

The Archive Settings dialog box appears.

Step 2 Enter the new location in the Archive Location field, or click **Browse** to select a directory on your system.

Step 3 Click **Apply** to accept the change to the default directory location.

Contract Connection

This section provides the FAQs and troubleshooting information for the Contract Connection application:

- Contract Connection FAQs
- Troubleshooting Contract Connection

Contract Connection FAQs

Q. Why does the Contract Status Detailed Report show no records for a valid contract?

A. You may need to refresh the Contract Status Detailed Report page. It might take some time to display the report. This is because of slow Cisco.com response.

Q. Why do I encounter an Invalid Credentials error message while generating a Contract Connections report with valid credentials?

A. You may have contracts but they may not be associated with your user ID. To ensure this, check whether you have Cisco Service contracts registered with your Cisco.com user ID by accessing the Cisco - Service Contract Center URL:

www.cisco.com/public/scc

If you encounter the following message:

```
Currently you have no Cisco Service contracts registered to your Cisco.com User Id
```

Then it means that your contracts are not registered to your Cisco.com User ID.

To ensure that your contracts are registered, place a request to add your Cisco.com contracts in Service Contract Center. Contact Cisco TAC (Technical Assistance Center) for more information on how to proceed with placing a request to register your contracts with Cisco - Service Contact Center. After placing a request with Cisco - Service Contract Center, access the Cisco - Service Contract Center again and verify if the contracts are registered. After successful verification, proceed to generate a Contract Connections report.

Troubleshooting Contract Connection

Message ID	Error Message	Probable Cause	Possible Action
CCX0001	No device selected.	You may not have selected any device.	Select one or more devices and continue to generate the report.
CCX0002	Cisco.com user credentials are not valid.	You may not have entered valid Cicso.com credentials.	Enter correct Cisco.com credentials.
CCX0003	You have entered a past date/time for creating the job.	You have entered a past date or time for creating a job.	Schedule this job to run either immediately or at a future date and time.
CCX0004	Problem with posting and getting the results from Cisco.com. Try again later.	This may be caused by a problem while connecting to Cisco.com or with Cisco.com, itself.	Check the User Guide for more details on how to correct this.

APPENDIX **B**

Understanding Syslog Formats

Devices are expected to comply with the following rules while sending syslogs:

- Device should include PRI as recommended by RFC 3164
- Device could optionally send Timestamp information in RFC recommended format in the header. The RFC recommendation does not include the TIMEZONE information. Hence, it is assumed that the device sends the local time and that the device and Server are in the same time zone.
- Device could optionally send Hostname information in the header.
- To support devices that are in different time zones than the server, IOS allows configuring the devices to send the Time Information along with TZ, optionally, in the message part of the syslog packet.

  Such timestamps should be prefixed with some separator character (like * or :), so the syslog daemons (such as unix syslogd) do not treat them as header information. This could cause unix syslogd to misinterpret the time information, because they ignore the TZ part of the Timestamp.

  Considering the above, devices should send syslogs in one of the following formats:

Format A

```
<187> [timestamp in RFC prescribed format] [device dns name | ip address] [Dummy
Value/Counter : ] [ {:|*} mmm dd hh:mm:ss TimeZone ]
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: description
```

Format B

```
<187> [timestamp in RFC prescribed format] [device dns name | ip address] [Dummy
Value/Counter : ] [ {:|*} yyyy mmm dd hh:mm:ss TimeZone <-|+> hh:mm]
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: description
```

```
Examples of good syslog messages: [ as sent by the device ]

<187>%PIX-4-106023 description

<187>Mar 23 10:21:03 %PIX-4-106023 description

<187>*Mar 23 12:12:12 PDT %PIX-4-106023 description

<187>Mar 23 10:21:03 *Mar 23 12:12:12 PDT %PIX-4-106023 description

<187>Mar 23 10:21:03 *2003 Mar 23 12:12:12 PDT  -8:00 %PIX-4-106023 description

<187>Mar 23 10:21:03 93: *2003 Mar 23 12:12:12 PDT  -8:00 %PIX-4-106023 description
```

The device ensures that the device IP address or DNS name if defined is maintained in the message header as the source IP address or source DNS name irrespective of the interface out of which the syslog message is sent.

The syslog message is sent on the network to the NMS (Network management station) using UDP. The UDP socket sent to, will be the UDP socket for syslog (514).

The payload of the message will be preceded by the logging facility code enclosed in angle braces (<>) that the receiving Syslog daemon uses for routing the message. Logging facility at the logging system is mapped to a log file on the system. The logging facility codes map as follows:

- (5<<3) = Syslog
- (23-16<<3) = Local 0 to Local 7

The combination FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC must be UNIQUE for a given message, so that Syslog Analyzer can provide non-trivial syslog support.

See the section, Enabling and Tracking Syslogs Using Syslog Analyzer and Collector for details.

APPENDIX **C**

RME Command Reference

This appendix provides a list of the RME commands.

Command	Description
`backup.pl`	Backs up the database. *NMSROOT*`/bin/perl backup.pl` *backdir* [*logfilename* [*numberGen*]]
`dbpasswd.pl`	Changes the database password along with its access configuration files. *NMSROOT*`/bin/dbpasswd.pl` {`all` | `dsn=`*data source* [`opwd=`*old password*] [`pfile=`*properties file*] | `listdsn`}
`dbRestoreOrig.pl`	Re-initializes the RME data (database and file system), if the RME data is corrupted and the database restore operation has failed. Syntax: *NMSROOT*`/bin/perl` *NMSROOT*`/bin/dbRestoreOrig.pl` `dsn=`*dsnname* `dmprefix=`*dmprefixname* [`npwd=`*newpassword*] Where: `dsn=`*xxx* *xxx* is the ODBC data source name for the database For Common Services, `dsn=`**`cmf`** For RME, `dsn=`**`rmeng`** `dmprefix` is required for constructing database engine process name. For Common Services, `dmprefix=`**`Cmf`** For RME, `dmprefix=`**`RME`** All the user configurable variable parameters are case-sensitive. Ensure that you enter the exact value as mentioned here—if not, the database will get corrupted.

Command	Description
`dig`	Sends domain name query packets to name servers. Dig (domain information groper) is a flexible command line tool which can be used to gather information from the Domain Name System servers. *Dig* has two modes: • Simple interactive mode which makes a single query • Batch which executes a query for each in a list of several query lines. All query options are accessible from the command line. *NMSROOT*/**bin/dig** [@server] *domain* [*query-type*] [*query-class*] [+*query-option*] [-*dig-option*] [%comment]
`dmgtd`	Process manager daemon. Specify the tcp port to use the Daemon Management protocol on. All clients will need to have the env var PX_DMGTHOST and env var set. Daemon Manager Protocol enabled applications can report additional status. Daemon Manager sends status information to Syslog (facility: LOG_DAEMON). *NMSROOT*/**bin/dmgtd** [**-p** *port* **-v**] [*names*]
`pdexec / pdshow / pdterm`	Controls process manager. *NMSROOT*/**bin/pdshow** *[appName1 appName2 ...]* *NMSROOT*/**bin/pdexec** *[appName1 appName2 ...]* *NMSROOT*/**bin/pdterm** *[appName1 appName2 ...]* • To get status of registered processes appName1, appName2, ..., send a request to CRM process manager using the command: **pdshow** *[appName1 appName2 ...]* • To start the registered process appName1 if it is not running, send a request to CRM process manager using the command: **pdexec** *appName1* • To stop the registered application appName1 if it is running send a request to CRM process manager using the command: **pdterm** *appName1* **pdshow** will show the status of all processes registered if no arguments are given. **pdexec** and **pdterm** require one or more *appNames*. where *appNameN* represents the registered name of each process that is registered with CRM process manager.
`pdmsg`	Broadcasts a string to all registered daemons under Daemon Management that are in the “Running Normally” state. To use this command, Daemon Management server must be running. *NMSROOT*/**bin/pdmsg** *msg-string*

Command	Description
`pdreg`	Registers and unregisters applications with CRM Process Manager. *NMSROOT*`/bin/pdreg [-r` *appName* `-e pgm [-f` *pgmFlags* `] [-d` *dependencies* `] [-n] [-t 0|p|n ] ]|[-u` *appName* `]|[-l` *appName* `]` • To register a process and invoke it without the **-n** or **-t** option. `pdreg -r` *appName* *appName* must be 25 alphanumeric characters or less. • To unregister a process and shut it down if the process is running. `pdreg -u` *appName* • To list the registry for a particular daemon. `pdreg -l` *appName*
`pdrun.pl`	A wrapper to run a command-line instruction within the CiscoWorks environment. The command line instruction to be run needs to be double quoted as the argument. If the command-line instruction itself contains double quotes, precede it with a back slash. To run a command line instruction within the CiscoWorks environment: *NMSROOT*`/bin/perl pdrun` **“pdshow \“ANIServer jrm\””**
`removeJrmJobs.pl`	Removes all the existing JRM jobs from cmf database. This is used in remote upgrade from RME 3.5.x and RME 3.4.x. *NMSROOT*`/rigel/scripts/rme/removeJrmJobs.pl`
`restorebackup.pl`	Restores an earlier backup of the database. *NMSROOT*`/bin/perl` *NMSROOT*`/bin/restorebackup.pl` [`-d` *BackupDirectory*] [`-gen` *GenerationNumber*] [`-t` *TempDirectory*] [`-help`] Where: • NMSROOT is the CiscoWorks installation directory • [`-d` *BackupDirectory*] Directory where RME 3.4 or RME 3.5 backup data is available. This is mandatory. • [`-gen` *GenerationNumber*] Version to be migrated to RME 4.1. By default, it will restore the latest backup data. If generations 1 through 5 exist, then 5 will be the latest. This is optional. • [`-t` *TempDirectory*] Temporary directory used by restore framework to extract the content of backup archive. By default the temporary directory is created under NMSROOT as *NMROOT*/tempBackupData. You can customize this, by using this `-t` option, where you can specify your own temp directory. This is to avoid overloading NMSROOT. This will be deleted after the data restoration is complete. This is optional. • [`-help`] Provides help. When used with `-d` *Backup Directory* syntax, shows correct syntax along with available suites and generations.
`uninstall.sh`	Uninstallation program that removes files and settings. Uninstallation allows you to remove only RME or remove CiscoWorks CD One as well. To remove CD One, you must remove RME as well. Before removing RME, you must first remove any applications that depend on RME. *NMSROOT*`/bin/uninstall.sh`

APPENDIX D

Managing Devices When RME Server is Within a NAT Boundary

This section introduces Network Address Translation (NAT) support in Resource Manager Essentials (RME) and gives details of the tasks that you need to perform, to enable support.

When the RME server is assigned an IP address that is within a NAT boundary, all the devices that are outside this boundary, cannot reach the RME server using the inside address of the RME server.

Such devices should use the translated outside address of the RME server as configured in the NAT, to successfully connect to the RME server for all device initiated operations such as:

- Sending syslogs
- Sending traps
- Initiating copy tftp operations from the device through command lines, etc.

Configuring RME Server for the NAT Environment

RME initiates file transfers from the device, while archiving configuration files from the device, or while transferring software images to and from the device.

During these operations, RME uses its own default address as the destination or the source for transfers, by default. The inside address of the RME Server is not reachable from the devices that are on the outside. For such devices, RME must use the correct outside address of its server for these transfers.

To do this, RME allows you to configure the outside address of its server (called Natted RME IP Address) for each device.

Managing Devices Outside the NAT Boundary

When all the devices being managed are outside the NAT boundary, you can configure a default Natted RME IP Address that you can use with these devices:

Step 1 Navigate to **Resource Manager Essentials > Admin > System Preferences.**

Step 2 Select RME Device Attributes from the TOC.

The RME Device Attributes dialog box appears.

Step 3 Enter the Natted RME IP Address in this dialog box.

This is the public, or the outside IP address of the RME server.

Only those devices that are added to the system after the default is set, will use the new Natted RME IP Address value.

All existing devices will have to be edited using this procedure to set the Natted RME IP Address value when a part of the network is outside the NAT boundary:

Step 1 Navigate to **Resource Manager Essentials > Device Management > RME Devices.**

The RME Devices dialog box appears.

Step 2 Select the required devices.

Step 3 Click **Edit Device Attributes**.

For the complete procedure to change the RME ID, see the topic Editing RME Device Attributes in the section Adding and Troubleshooting Devices Using Device Management.

When you configure devices that are outside the NAT boundary, for Syslog and trap destinations using NetConfig templates, you must use the translated outside address of the receiving server as the destination address.

INDEX

A

access
  privileges for NetConfig jobs, assigning 9-4
  Telnet and SSH, configuring 12-45
Adhoc task, in NetConfig
  about 9-32
  using 9-26
alias devices, managing 3-36
  about 3-36
  resolving 3-37
applications
  Audit Trail 15-1
  Bug Toolkit 16-1
  Change Audit 13-1
  Config Editor 10-1
  Configuration Management 8-1
  Contract Connection 18-1
  Inventory 6-1
  Job Approval 20-1
  NetConfig 9-1
  NetShow 11-1
  SmartCase 17-1
  Software Management 12-1
  Syslog Analyzer and Collector 14-1
  task overviews (tables) 2-1
    Bug Toolkit 1-15
    Change Audit and Audit Trail 1-16
    Config Editor 1-10
    Configuration Management 1-9
    Device Management 1-7
    Inventory 1-6
    Job Management and Job Approval 1-13
    NetConfig 1-11
    Reports 1-14
    Software Management 1-12
    Syslog Analyzer and Collector 1-17
  what's new and RME task overviews (tables) 2-1
Archive Management (part of Configuration Management) 8-1
  about 8-1
  archive purging 8-29
  archive searches 8-50
  archive status, checking 8-31
  configurations, modifying 8-5
  credentials, entering 8-4
  custom search queries
    creating 8-51
    deleting 8-53
    editing 8-53
    running 8-52
  search report, displaying 8-54
  security, modifying 8-7
    Catalyst commands 8-7
    content engine commands 8-8
    content service switch commands 8-8
    IOS commands 8-7
  setting up 8-20
    directory, moving 7-10, 8-20
    shadow directory, enabling and disabling 8-21
  using 8-4
Archiving netshow job output 11-15
audience for this document i-xxxi
Audit Trail, using 15-1
  about 15-1
  standard report, generating 15-5

Audit Trail application
  task overview (table) 1-16
Authentication Proxy task in NetConfig 9-33
authorizing a distribution job, in Software Management 12-54
automated actions, defining
  in Change Audit 13-8
    creating 13-9
    deleting 13-13
    editing 13-11
    enabling, disabling 13-12
    exporting, importing 13-12
  in Syslog Analysis 14-29
    creating 14-30
    deleting 14-35
    editing 14-32
    enabling, disabling 14-34
    example of 14-36
    exporting, importing 14-35
    verifying 14-37

B

backup.pl command, description C-1
backup policy, setting 14-19
Banner task in NetConfig 9-34
baseline configurations 8-73
  Baseline Compliance report 8-98
  Baseline Configs window 8-76
  commands, deploying 8-99
  compliance jobs, deleting 8-103
  non-compliance report, running 8-96
baseline configuration templates 8-77
  (see also baseline configurations) 8-73
  creating
    advanced 8-78
  deleting 8-88
  editing 8-86
  exporting 8-87
  importing 8-87
Bug Toolkit, using 16-1
  Bug Summary report
    generating 16-1
    understanding 16-3
  Cisco.com, logging into 16-3
  Locate Device report
    generating 16-4
    understanding 16-7
  troubleshooting A-99
Bug Toolkit application
  task overview (table) 1-15

C

CA (Certification Authority) task in NetConfig 9-37
Cable BPI/BPI+ task in NetConfig 9-79
Cable DHCP-GiAddr and Helper task in NetConfig 9-80
Cable Downstream task in NetConfig 9-82
Cable Interface Bundling task in NetConfig 9-87
Cable Spectrum Management task in NetConfig 9-88
Cable Trap Source task in NetConfig 9-90
Cable Upstream task in NetConfig 9-84
Catalyst devices
  1900/2820 device upgrade recommendations 12-85
  configuring using Telnet 14-14
  upgrade recommendations, understanding 12-84
cautions
  significance of i-xxxi
cautions regarding
  changing Change Audit purge settings 13-4, 15-8
  NetConfig's Adhoc task 9-32
  NetConfig commands in a user-defined template 9-19
  resetting purge policy in Syslog Analyzer 14-20
CDP task in NetConfig 9-35
CE (Content Engine) devices
  configuring using Telnet 14-15
Change Audit, using 13-1
  automated actions, defining 13-8

        Automated Action window details 13-9
        creating 13-9
        deleting 13-13
        editing 13-11
        enabling, disabling 13-12
        exporting, importing 13-12
    exception periods
        creating 13-7
        defining 13-6
        deleting 13-8
        editing 13-8
        enabling and disabling 13-7
    maintenance tasks 13-3
        forced purges, performing 13-4, 15-8
        purge policy, setting 13-3, 15-7
    overview
        Syslog, comparison with 13-1
    process
        about 13-20
        stopping and starting 13-21
    report details 13-19
    reports 13-13
        Exception Period report 13-14
        standard report 13-16
    troubleshooting A-97
Change Audit application
    task overview (table) 1-16
CIP microcode image types, and software image upgrades 12-53
Cisco.com
    adding images from 12-19
    Software Management tasks, and 12-4
    software repository, synchronizing with 12-31
Cisco IOS device upgrade recommendations 12-84
CiscoWorks Server, and Software Management 12-3
CLI utilities
    cwcli 19-1
        inventory CDA job commands
            createjob 19-80
            deletejob 19-81
            jobdetails 19-81
            jobresults 19-82
            listjobs 19-82
            stopjob 19-81
    profiles and PTT 19-105
    PTT 19-105
        commands 19-107
    PTT features 19-105
    SWIMcli 19-110
        execute SWIM cli remotely 19-113
        running swim cli commands 19-110
    syslogConf 19-108
    syslogConf.pl utility 19-108
CLI utilities(see cwcli config) 19-1
command reference
    (see also cwcli config, using) 19-1
    backup.pl C-1
    command-line tool
        see cwcli netconfig command 9-91
    dbpasswd.pl C-1
    dbRestoreOrig.pl C-1
    dig C-2
    dmgtd C-2
    pdexec C-2
    pdmsg C-2
    pdreg C-3
    pdrun.pl C-3
    pdshow C-2
    pdterm C-2
    RemoveJrmJobs.pl C-3
    restorebackup.pl C-3
    RME commands C-1
    uninstall.sh C-3
Common Syslog Collector (see under Syslog Analyzer) 14-1
config_DeployBaselinTempUI 8-89
Config CLI, troubleshooting A-101
Config Editor
    editor manager, working with

    - in processed mode 10-9
- Config Editor, using
  - benefits of 10-2
  - changes in this release 10-7
  - configuration files
    - closing 10-18
    - downloading 10-30
    - editing 10-8
    - exporting to HTML format 10-15
    - opening 10-24
    - removing 10-12
    - saving 10-12
  - configuration restore operation 10-30
  - configuration tools 10-18
    - to check syntax 10-21
    - to compare versions 10-19
    - to display changes 10-20
  - device states, and 5-6
  - downloading configuration files 10-30
    - files, selecting 10-31
    - job password policy 10-39
    - job scheduling 10-32
    - job status, viewing 10-39
    - starting a job 10-31
    - work orders, reviewing 10-38
  - editor manager, working with 10-8
    - Config Editor, using jobs, in 10-10
    - credentials, modifying with 10-11
    - processed mode 10-9
  - open files, viewing list of 10-23
  - opening a file 10-24
    - by device and version 10-24
    - from an external location 10-28
    - viewing a list of open files 10-23
  - preferences, setting up 10-7
  - printing a file 10-15
  - restore operation 10-30
  - search and replace in configuration files 10-14
  - tasks in 10-1
  - undoing all edits 10-13
- Config Editor application
  - task overview (table) 1-10
  - troubleshooting A-30
- configuration files
  - changes to
    - displaying 10-20
  - closing 10-18
  - currently open, viewing list of 10-23
  - downloading 10-30
    - files, selecting 10-31
    - job password policy 10-39
    - job scheduling 10-32
    - job status, viewing 10-39
    - starting a new job 10-31
    - work orders, reviewing 10-38
  - editing 10-8
  - exporting to HTML format 10-15
  - opening 10-24
    - by baseline 10-27
    - by device and version 10-24
    - by pattern search 10-25
    - external files 10-28
  - printing 10-15
  - removing 10-12
  - saving 10-12
  - syntax checking 10-21
    - about 10-21
    - external interface 10-21
  - versions of, comparing 10-19
- Configuration Management, using 8-1
  - administrator tasks 8-3
  - archival reports 8-32
    - Failed Devices report 8-33
    - Partially Successful Devices report 8-33
    - Successful Devices report 8-32
  - Archive Management (see Archive Management) 8-1
  - Archive Management Job Browser 8-65
    - deleting a job 8-71

    - job details, viewing 8-72
    - retrying a job 8-68
    - stopping a job 8-70
- archive purging 8-29
- archive searches with custom queries 8-50
    - creating queries 8-51
    - deleting queries 8-53
    - editing queries 8-53
    - running queries 8-52
    - search report, displaying 8-54
- archive status, checking 8-31
- baseline configurations (see baseline configurations) 8-73
- collection settings, defining 8-26
- comparing configurations 8-59
    - Config Diff Viewer 8-63
    - running versus latest archived 8-60
    - startup versus running 8-59
    - two versions of different 8-61
    - two versions of same 8-60
- Config Editor option
    - functional flow (figure) 10-2
    - tasks (table) 10-3
- configuration version tree 8-39
- Config Viewer 8-40
- job policies, configuring 8-14
    - defining default policies 8-14
    - scenarios, job password configured 8-17
- job scheduling
    - Sync Archive 8-34
    - Sync on Device 8-37
- labels, configuring 8-46
    - creating 8-47
    - deleting 8-50
    - editing 8-48
    - purging 8-50
    - viewing 8-49
- Quick Configuration Download feature
    - about 8-39
        - using 8-44
    - reports
        - archive search report 8-54
        - Configuration Version summary 8-42
        - Device Configuration Quick View 8-56
        - Out-of-Sync report 8-36
        - Search Archive Result 8-55
    - transport protocols, configuring 8-9
        - order, defining 8-13
        - requirements for use 8-10
    - troubleshooting A-21
- Configuration Management application
    - task overview (table) 1-9
- conflicting device types, working with 3-38
    - deleting the conflicting type 3-40
    - resolving the type conflict 3-39
- Contract Connection
    - accessing and using 18-1
    - reports
        - contract status detailed 18-2, 18-4
        - device type summary 18-2
        - generated, archiving and viewing 18-8
    - scheduling jobs 18-6
        - viewing job status 18-7
    - working with 18-1
- Creating netshow jobs 11-7
- Crypto Map task in NetConfig 9-38
- CSS (Content Service Switch) devices
    - configuring using Telnet 14-15
- cwcli config, using 19-1
    - batch processing 19-2, 19-7
    - CLI framework 19-2, 19-7
    - command parameters 19-11
        - all commands 19-11
        - compare command 19-11
        - delete command 19-11
    - core options and nmconfig equivalents 19-17
    - examples of cwcli config and nmconfig equivalents 19-18

- getting started 19-7
- man page information 19-18
  - arguments and options, about 19-19
  - function-dependent options 19-20
  - function-independent options 19-20
  - function-specific options 19-20
  - input list file format 19-22
  - mandatory arguments 19-19
  - -view option usage 19-23
- man page information for subcommands 19-23
  - compare 19-24
  - compareanddeploy 19-24
  - comparewithbaseline 19-25
  - delete 19-25
  - deploybaseline 19-25
  - export 19-26
  - get 19-26
  - import 19-27
  - listlock 19-27
  - put 19-27
  - reload 19-28
  - run2start 19-28
  - start2run 19-28
  - write2run 19-29
  - write2start 19-29
- overview 19-2, 19-7
- running 19-10
  - additional information 19-11
  - on multiple devices 19-10
- syntax examples 19-14
- uses 19-8
  - comparing configurations 19-10
  - deleting configurations 19-9
  - device and archive updates 19-8
  - remote access 19-10

cwcli netconfig command 9-91
- man page 9-91

D

dbpasswd.pl command, description C-1

deleting
- device groups 4-10
- devices
  - conflicting types 3-40
  - normal 3-22
  - pre-deployed 3-30
  - suspended 3-27
- images from the software repository 12-32

device groups, managing 4-1
- administering groups 4-16
- creating 4-3
  - group properties, entering 4-3
  - group rules, defining 4-5
  - membership, assigning 4-6
  - summary, displaying 4-7
- deleting 4-10
- details, viewing 4-8
- Device Management task overview (table) 1-7
- editing 4-8
- grouping rules, understanding 4-11
- membership
  - refreshing 4-10
  - viewing 4-9
- RME Group Administration page 4-2

devices
- outside the NAT, managing D-1
- syslog messages for, not getting A-91

devices, managing
- adding
  - automatically 3-12
  - manually 3-8
- alias devices 3-36
  - about 3-36
  - resolving 3-37
- attributes, editing 3-12

  - bugs filed against, identifying (see Bug Toolkit application) 16-1
  - configurations, verifying 9-2
  - conflicting device types 3-38
    - deleting the conflicting type 3-40
    - resolving the type conflict 3-39
  - credentials, verifying 9-2
  - device credentials
    - viewing 3-40
  - device manageability status 3-67
  - Device Management task overview (table) 1-7
  - Device Selector 3-68
    - device icons and types 3-79
    - displaying available devices 3-76
    - selecting a device 3-79
  - images from, adding to the software repository 12-22
  - normal devices, managing 3-20
    - deleting 3-22
    - exporting 3-21
    - resubmitting 3-23
    - suspending 3-21
  - pending devices, working with 3-24
  - pre-deployed devices, managing 3-27
    - deleting 3-30
    - exporting 3-28
    - resubmitting 3-31
    - suspending 3-29
  - prompts, verifying 9-3
  - states, viewing 3-19
  - suspending devices, managing 3-25
    - deleting 3-27
    - resubmitting 3-26
- devices, working with 3-1
- device security, modifying 9-3
- Device Selector
  - device icons and types 3-79
  - displaying available devices 3-76
  - filtering usage example 3-75
  - selecting a device 3-79
- device selector 3-68
- dig command, description C-2
- dmgtd command, description C-2
- DNS task in NetConfig 9-40
- documentation i-xxxi
  - audience for this i-xxxi
  - related to this product i-xxxiii
  - typographical conventions in i-xxxi
- downloading configuration files 10-30
  - files, selecting 10-31
  - job password policy 10-39
  - job scheduling 10-32
  - job status, viewing 10-39
  - starting a job 10-31
  - work orders, reviewing 10-38

E

- editing device groups 4-8
- editor manager (see under Config Editor) 10-8
- Enable A-23, A-24
- Enable Password task in NetConfig 9-41
- exporting
  - automated actions in Syslog Analysis 13-12
  - configuration files, to HTML format 10-15
  - devices
    - normal 3-21
    - pre-deployed 3-28
  - message filters, in Syslog Analyzer 14-40

F

- files
  - configuration (see configuration files) 10-8
  - Software Management, locating 12-95
- filters
  - Inventory change report filters, setting 6-12
  - Inventory change report filters, setting, Collection or Polling schedule, changing 6-11

- message filters in Syslog Analyzer, defining 14-38
  - creating 14-38
  - deleting 14-41
  - editing 14-39
  - enabling, disabling 14-40
  - exporting, importing 14-40
- forced purges
  - in Change Audit 13-4, 15-8
  - in Syslog Analyzer 14-21

H

- How A-21
- HTML format, exporting a configuration file to 10-15
- HTTP, configuring for software image upgrades 12-53
- HTTP Server task in NetConfig 9-43

I

- IGMP Configuration task in NetConfig 9-47
- IKE (Internet Key Exchange) Configuration task in NetConfig 9-50
- images
  - adding to software repository 12-19
    - from a file system 12-25
    - from a URL 12-26
    - from Cisco.com 12-19
    - from devices 12-22
    - from the network 12-28
  - attributes 12-33
    - default attribute values, understanding 12-34
    - editing and viewing 12-35
    - finding missing attribute information 12-35
    - understanding 12-34
  - deleting 12-32
  - distribution by 12-64
  - IOS images, and recommendation filters 12-11
  - searching for 12-33
- importing automated actions in Syslog Analysis 13-12
- Interface IP Address Configuration task in NetConfig 9-49
- Inventory 1-6
  - change report filters, setting 6-12
- Inventory, using 6-1
  - change report filters, setting 6-11
  - collection or polling schedule, changing 6-22
  - data, collecting and updating 6-2
  - graphs, generating 6-3
  - Inventory Job Browser 6-4
    - collection jobs, creating and editing 6-8
    - job details, viewing 6-7
    - polling jobs, creating and editing 6-8
  - prerequisites 6-2
  - prerequisites for use 6-2
  - reports, generating 6-24
    - 24 hour inventory change report 6-28
    - chassis slot details 6-31
    - chassis slot summary 6-31
    - chassis summary graph 6-33
    - detailed device report 6-30
    - EOS, EOL report 6-35
    - Hardware report 6-29
    - hardware summary graph 6-32
    - multiservice port details 6-31
    - PSIRT summary report 6-33
    - Software report 6-29
    - software version graph 6-32
  - reports, viewing 6-3
  - reports and graphs, viewing 6-3
  - report templates, working with 6-38
    - creating 6-38
    - deleting 6-44
    - modifying 6-43
    - running 6-44
  - task overview (table) 1-6
- Inventory Reports, troubleshooting A-15
- IOS
  - devices, configuring

        using Telnet 14-14
    images, and recommendation filters 12-11

J

Job Approval
    task overview (table) 1-13
Job Approval, using 20-1
    approver details, specifying 20-2
    approver lists
        assigning 20-4
        creating, editing 20-3
    jobs, approving and rejecting 20-5
    jobs, enabling 20-8
    setting up 20-4
    task workflow 20-2
    troubleshooting A-97
Job Browser (see under Inventory) 6-4
Job Browser and Collection Status 6-4

L

Local Username task in NetConfig 9-44
Login A-22, A-23

M

managing devices
    RME within NAT boundary D-1
Masking credentials of show commands 11-7
message filters, in Syslog Analysis 14-38
    creating 14-38
    deleting 14-41
    editing 14-39
    enabling, disabling 14-40
    exporting, importing 14-40
MICA portware image types, and software image upgrades 12-53
microcode and modem firmware requirements for software image upgrades 12-53
Microcom firmware image types, and software image upgrades 12-53
Modifying a Custom Template 6-43

N

NAT (see under devices) D-1
NetConfig
    task overview (table) 1-11
NetConfig, using 9-1
    before you begin 9-2
        device configurations, verifying 9-2
        device credentials, verifying 9-2
        device prompts, verifying 9-3
        device security, modifying 9-3
        job approval, enabling 9-4
        job policies, default, configuring 9-3
        task access privileges, assigning 9-4
    cwcli netconfig command description 9-91
    device states, and 5-7
    interactive commands, handling 9-26
        .ini file 9-27
        user-defined templates 9-26
    job, starting a new 9-6
    job approvers, setting 9-18
    job password 9-18
    job policies, default, configuring 9-18
    jobs, browsing and editing 9-11
        job details, viewing 9-15
    multi-line commands, handling 9-27
    rolling back configuration changes 9-4
        rollback commands, creating 9-4
        rollback on failure, configuring 9-4
    system-defined tasks 9-27
        Adhoc tasks 9-32
        Authentication Proxy task 9-33
        Banner task 9-34

        Cable BPI/BPI+ task 9-79
        Cable DHCP-GiAddr and Helper task 9-80
        Cable Downstream task 9-82
        Cable Interface Bundling task 9-87
        Cable Spectrum Management task 9-88
        Cable Trap Source task 9-90
        Cable Upstream task 9-84
        CDP task 9-35
        Certification Authority (CA) task 9-37
        Crypto Map task 9-38
        dialog box, understanding 9-30
        DNS task 9-40
        Enable Password task 9-41
        HTTP Server task 9-43
        IGMP Configuration task 9-47
        IKE Configuration task 9-50
        Interface IP Address Configuration task 9-49
        Local Username task 9-44
        NTP Server Configuration task 9-52
        RADIUS Server Configuration task 9-53
        RCP Configuration task 9-56
        Reload task 9-57
        SNMP Community Configuration task 9-58
        SNMP Security Configuration task 9-60
        SNMP Traps Configuration task 9-62
        SSH Configuration task 9-70
        Syslog task 9-67
        TACACS+ Configuration task 9-73
        TACACS Configuration task 9-72
        Telnet Password Configuration task 9-75
        Transform task 9-76
        User-Defined Protocol task 9-78
        Web User task 9-77
    tasks 9-1
    tasks, assigning to users 9-25
    templates 14-16
    transport protocol order for jobs, setting 9-18
    troubleshooting A-28
    user-defined tasks, creating and editing 9-18
    user permissions, understanding 9-5
        administrator task permissions 9-5
        job approval permissions 9-5
        job editing permissions 9-5
        user-defined task permissions 9-5
NetShow
    adding and deleting adhoc commands 11-22
    Administering NetShow settings 11-26
        assigning approval lists 11-31
        defining default job policies 11-27
        defining protocol order 11-29
        generating standard audit trail report 11-32
        purging jobs 11-28
        setting log levels 11-30
    archiving job output 11-15
    Commands
        adding and deleting adhoc commands 11-22
        custom command execution privilege, assigning 11-23
        cwcli netshow command 11-26
        launching show commands from device center 11-24
        using show commands 11-1
    Command Sets 11-17
        assigned Command Sets, showing 11-23
        assigning 11-22
        assigning to users 11-23
        command set details, viewing 11-19
        creating 11-19
        deleting 11-21
        editing 11-20
        managing 11-19
        system-defined command sets 11-18
    credentials, masking 11-7
    Deleting output atchive 11-17
    Job Work Order 11-9
    NetShow job browser 11-3
        copying jobs 11-13
        creating jobs 11-7

- deleting jobs 11-14
- editing jobs 11-10
- job details, viewing 11-5
- stopping jobs 11-13
- NetShow jobs,working with 11-2
- viewing job output 11-15
- viewing permission report 11-2

Netshow
- Working with NetShow Jobs 11-2

NTP Server Configuration task in NetConfig 9-52

O

overviews
- Common Syslog Collector 14-4
- editing a configuration file in Config Editor 10-8
- of cwcli config 19-2, 19-7
- opening a configuration file 10-24
- RME 1-1
- syntax checking in Config Editor 10-21
- Syslog Analyzer 14-4
- Syslog Analyzer reports 14-41

P

pdexec command, description C-2

pdmsg command, description C-2

pdreg command, description C-3

pdrun.pl command, description C-3

pdshow command, description C-2

pdterm command, description C-2

PIX Firewall devices, upgrade recommendations, understanding 12-86

purging messages
- cautions regarding changing purge values
  - in Change Audit 13-4, 15-8
  - in Syslog Analyzer 14-20
- forced purges
  - in Change Audit 13-4, 15-8
  - in Syslog Analyzer 14-21
- purge policies, setting
  - in Change Audit 13-3, 15-7
  - in Syslog Analyzer 14-20

R

RADIUS Server Configuration task in NetConfig 9-53

rcp
- configuring for software image upgrades 12-47
  - on Solaris 12-47
  - selecting as active file transfer method 12-49
- RCP Configuration task in NetConfig 9-56

removeJrmJobs.pl command, description C-3

reports, generating 7-1
- archived reports
  - purging 7-8
  - viewing 7-7
- Audit Trail standard report 15-5
- Bug Toolkit reports
  - Bug Summary 16-1
  - Locate Device 16-4
- Change Audit reports
  - Exception Period 13-14
  - standard 13-16
- custom report templates 7-5
  - creating 7-6
  - deleting 7-6
  - editing 7-6
- report jobs, purging 7-8
- Reports Generator 7-4
- Reports Job browser 7-1
- Syslog Analyzer reports
  - Severity Level Summary 14-45
  - standard 14-46
  - Syslog 24-Hour Report 14-45
  - Syslog Custom Summary 14-45
  - Unexpected Devices 14-47

Reports task overview (table) 1-14

report templates in Inventory, working with 6-38
  creating 6-38
    adding rules 6-40
    deleting rules 6-43
    modifying rules 6-42
  deleting 6-44
  modifying 6-43
  running 6-44
restorebackup.pl command, description C-3
rolling back configuration changes in NetConfig 9-4
  rollback commands, creating 9-4
  rollback on failure, configuring 9-4
RSAC (Remote Syslog Analyzer Collector)
  properties file
    COLLECTOR_PORT 14-9
    COUNTRY_CODE 14-7
    DEBUG_CATEGORY_NAME 14-8
    DEBUG_FILES 14-8
    DEBUG_LEVEL 14-8
    DEBUG_MAX_BACKUPS 14-9
    DEBUG_MAX_FILE_SIZE 14-9
    FILTER_THREADS 14-9
    PARSER_FILE 14-9
    QUEUE_CAPACITY 14-9
    READ_INTERVAL_IN_SECS 14-9
    SUBSCRIPTION_DATA_FILES 14-9
    SYSLOG_FILES 14-8
    TIMEZONE 14-7
    TIMEZONE_FILE 14-8

S

searching for images 12-33
security warning regarding -p 19-20
Setting system preferences 21-1
  collection failure notification 21-9
  job purge 21-3
  log level settings 21-1
  RME device attributes 21-7
  RME secondary credentials 21-8
SmartCase
  launching CCO Service Request Tool 17-1
SNMP
  SNMP Community Configuration task in NetConfig 9-58
  SNMP Security Configuration task in NetConfig 9-60
  SNMP Traps Configuration task in NetConfig 9-62
Software Management
  task overview (table) 1-12
Software Management, using 12-1
  administration tasks 12-6
    preferences, viewing and editing 12-7
    upgrade information, updating 12-13
  distribution by devices 12-55
  distribution by images 12-64
  distribution job, authorizing 12-54
  environment, setting up 12-3
    Cisco.com, logging into 12-4
    CiscoWorks Server 12-3
  files, locating 12-95
  Job Approval 12-6
  patch distribution 12-69
    by device 12-70
    by patch 12-73
  preferences, viewing and editing 12-7
    protocol order, selecting 12-10
    recommendation filters, and IOS images 12-11
  remote staging and distribution 12-76
  software distribution 12-36
    methods 12-41
    upgrade analysis 12-37
    Upgrade Analysis report, understanding 12-39
    upgrades, configuring devices for 12-44, 12-51
    upgrades, planning 12-42
    upgrades from Cisco.com, planning 12-37
    upgrades from the software repository, planning 12-38
  software image repository, maintaining 12-43

- Software Management jobs 12-86
  - deleting 12-91
  - failed job, retrying 12-88
  - schedule, changing 12-88
  - stopping 12-90
  - succesful, undoing 12-89
- software repository 12-15
  - image attributes 12-33
  - images, adding 12-19
  - images, deleting 12-32
  - searching 12-33
  - synchronization 12-16
  - synchronization jobs, removing 12-18
  - synchronization report, scheduling 12-17
  - synchronization report, viewing 12-18
  - syncrhonizing with Cisco.com 12-31
- support for IOS software modularity 12-68
- troubleshooting A-32
- upgrade information, updating 12-13
  - before you begin 12-14
- upgrade recommendations, understanding 12-83
  - for Catalyst devices 12-84
  - for Catlyst 1900/2920 devices 12-85
  - for Cisco IOS devices 12-84
  - for PIX Firewall devices 12-86
  - for VPN 3000 series devices 12-85
- upgrades, scheduling 12-53
- user-supplied scripts, understanding 12-92

SSH Configuration task in NetConfig 9-70

states, managing 5-1
- RME 3.x behavior 5-1
- scenarios 5-5
  - adding a device 5-5
  - configuration changes 5-7
  - configuration deployment 5-6
  - Inventory detailed device report 5-6
  - software image upgrade 5-8
- state descriptions 5-2
- transitions 5-3
  - aliased 5-4
  - normal 5-4
  - pending 5-3
  - pre-deployed 5-4
  - suspended 5-4

syslog
- formats B-1

Syslog Analysis application
- FAQs on
  - location of syslog messages A-92
  - not getting syslog messages for devices A-91

Syslog Analyzer
- purge policy
  - caution regarding changing values 14-20
  - setting 14-20
- reports, generating
  - Severity Level Summary report 14-45
  - standard reports 14-46
  - Syslog Custom Summary report 14-45
  - Unexpected Device report 14-47
- reports, overview 14-41
- reports, understanding 14-44
- report templates (see Syslog Analyzer custom report templates) 14-22
- status, viewing 14-5, 14-13
  - collector status, viewing 14-5
  - procedure 14-6
- task overview (table) 1-17
- troubleshooting A-91
- workflow 14-10
  - stopping and restarting 14-12
  - UNIX, syslog configuration file on 14-12
  - Windows 2000 14-11

Syslog Analyzer and Collector, using 14-1
- automated actions 14-29
  - creating 14-30
  - deleting 14-35
  - editing 14-32
  - enabling, disabling 14-34

    example 14-36
    exporting, importing 14-35
  backup policy, setting 14-19
  Common Syslog Collector, subscribing to 14-5
    collector status, viewing 14-5
    procedure 14-6
  custom report templates
    defining 14-22
    deleting 14-26
    editing 14-26
  devices, configuring for 14-13
    before you begin 14-13
    using NetConfig templates 14-16
    using Telnet 14-14
  forced purges 14-21
  message filters 14-38
    creating 14-38
    deleting 14-41
    editing 14-39
    enabling, disabling 14-40
    exporting, importing 14-40
  overview 14-4
Syslog Analyzer custom report templates
  creating 14-23
    adding a message type 14-24
    deleting a message type 14-25
    editing a message type 14-25
    selecting a message type 14-26
  running 14-27
Syslog task in NetConfig 9-67
System-defined command sets 11-18

T

TACACS+ Configuration task in NetConfig 9-73
TACACS Configuration task in NetConfig 9-72
TACACS credentials, interpreting A-21
  custom TACACS prompts, troubleshooting A-24
  enable login authentication
    in SSH mode A-24
    in Telnet mode A-23
  login authentication
    in SSH mode A-23
    in Telnet mode A-22
task overviews (tables)
  Bug Toolkit 1-15
  change tracking 1-16
  configuration editing 1-10
  configuration management 1-9
  device and group management 1-7
  job management 1-13
  NetConfig 1-11
  reporting 1-14
  software management 1-12
  Syslog Analyzer and Collector 1-17
Telnet
  Telnet Password Configuration task in NetConfig 9-75
  using to configure devices for Syslog Analyzer 14-14
  using to configuring devices for Syslog Analyzer
    Catalyst devices 14-14
    CE devices 14-15
    CSS devices 14-15
Telnet, using to configure devices for Syslog Analyzer
  IOS devices 14-14
TFTP, configuring for software image upgrades 12-51
  on Solaris 12-51
  on Windows 12-51
Transform task in NetConfig 9-76
transport protocols, configuring 8-9
  order, defining 8-13
  requirements for use 8-10
troubleshooting A-1
  BugToolKit A-99
  Change Audit A-97
  Config CLI A-101
  Config Editor A-30
  Config Management A-21

    - Inventory Reports A-15
    - Job Approval A-97
    - NetConfig A-28
    - Software Management A-32
    - Syslog A-91
- typographical conventions in this document i-xxxi

U

- uninstall.sh command, description C-3
- upgrades
  - analyzing prerequisites and impact 12-37
  - configuring devices for 12-44
    - additional requirements, meeting 12-44
    - additional SFB checks 12-45
    - HTTP 12-53
    - microcode requirements 12-53
    - minimum requirements, meeting 12-44
    - modem firmware requirements 12-53
    - rcp, configuring 12-47
    - SCP, configuring 12-47
    - Telnet and SSH access, configuring 12-45
    - TFTP, configuring 12-51
  - distributing by devices
    - advanced 12-59
    - basic 12-55
  - distributing by images 12-64
  - distribution job, authorizing 12-54
  - distribution methods 12-41
  - planning 12-42
    - from Cisco.com 12-37
    - from the software repository 12-38
    - identifying possible changes 12-42
    - prerequisites, satisfying 12-42
    - software repository, maintaining 12-43
    - testing the new images 12-43
  - recommendations, understanding 12-83
    - for Catalyst 1900/2820 devices 12-85
    - for Catalyst devices 12-84
    - for Cisco IOS devices 12-84
    - for PIX Firewall devices 12-86
    - for VPN 3000 devices 12-85
  - remote staging and distribution 12-76
    - external TFTP server 12-77
    - remote stage device 12-77
  - scheduling 12-53
  - Upgrade Analysis report, understanding 12-39
- User-Defined Protocol task in NetConfig 9-78
- user-supplied scriptsfor software management 12-92

V

- viewing
  - Software Management synchronization reports 12-18
  - user-defined device groups
    - membership details 4-9
    - properties 4-8
- VPN 3000 devices, upgrade recommendations, understanding 12-85

W

- warnings
  - regarding security and -p 19-20
- warnings regarding
  - configuration change detection schedule, and purging 8-29
  - device passwords during export 3-17, 3-21, 3-29
- Web User task in NetConfig 9-77
- What A-24
- what’s new in this release
  - in Config Editor 10-7
- Windows, and the NetConfig .ini file 9-27